Servicios y cargas de trabajo del plano de control de IaaS de vSphere

Actualización 3

VMware vSphere 8.0
VMware vCenter 8.0
VMware ESXi 8.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Acerca de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*

1

Servicios y cargas de trabajo del plano de control de IaaS de vSphere, anteriormente denominado *Servicios y cargas de trabajo de vSphere with Tanzu* describe cómo prestar servicios y ejecutar cargas de trabajo en un entorno de espacio de nombres de vSphere en vSphere IaaS control plane, anteriormente conocido como vSphere with Tanzu. Puede obtener información sobre cómo crear un espacio de nombres e implementar cargas de trabajo como servicios de supervisor, máquinas virtuales y pods de vSphere.

Audiencia prevista

Esta información está destinada principalmente a administradores de vSphere que utilizan vSphere IaaS control plane para configurar y asignar recursos de vSphere a un espacio de nombres de vSphere de Supervisor. Posteriormente, diferentes servicios y cargas de trabajo que se ejecutan dentro del espacio de nombres pueden consumir estos recursos. Generalmente, los administradores de vSphere que utilizan vSphere IaaS control plane suelen tener conocimientos básicos sobre contenedores y otros conceptos de Kubernetes.

La guía también puede ser utilizada por los equipos de desarrollo y operaciones que deseen implementar cargas de trabajo como pods de vSphere, máquinas virtuales y servicios de supervisor en el Supervisor.

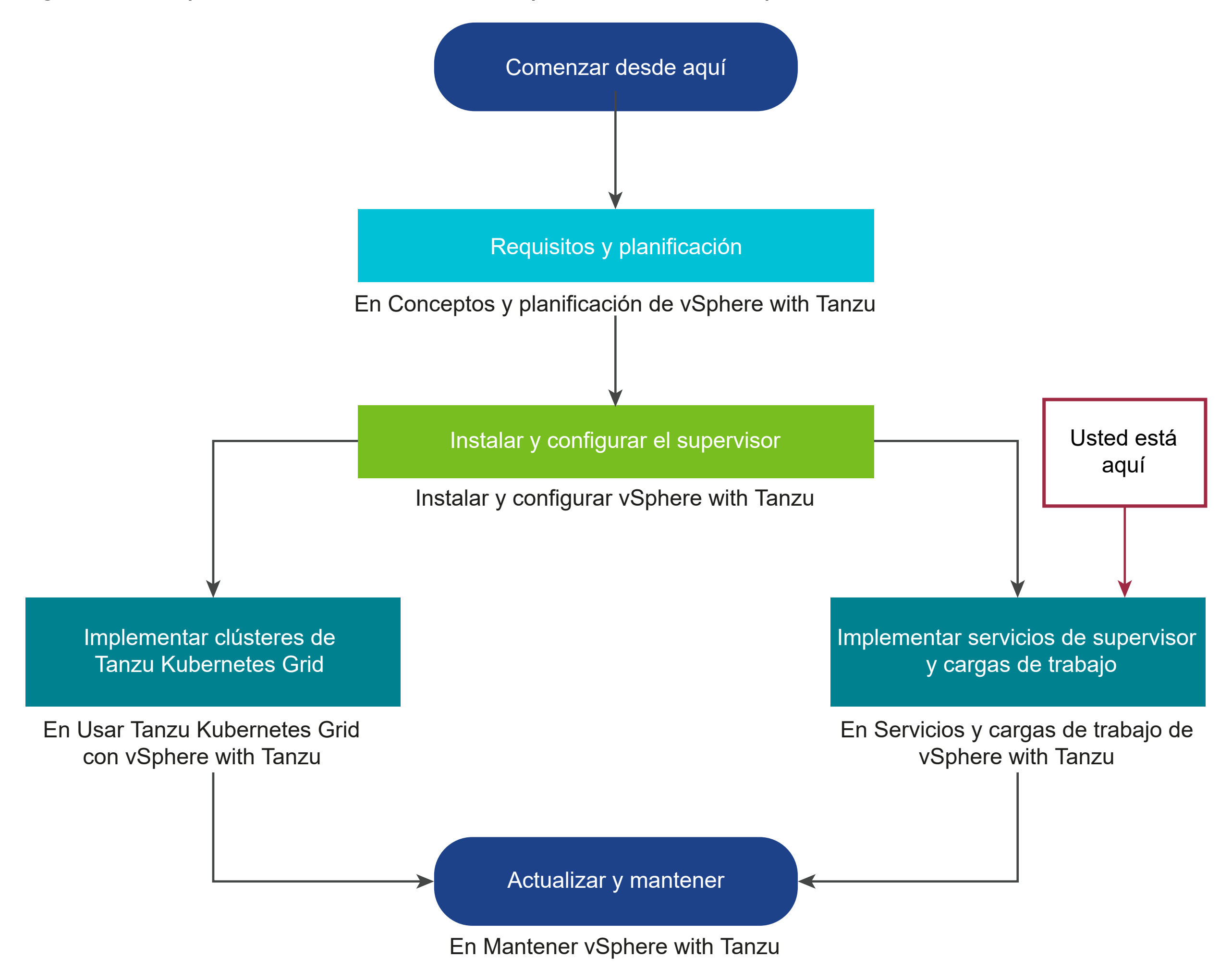
Nota *Servicios y cargas de trabajo del plano de control de IaaS de vSphere* no incluye información sobre las cargas de trabajo en ejecución en un clúster de Tanzu Kubernetes Grid. Para obtener información sobre cómo trabajar con clústeres de Tanzu Kubernetes Grid, consulte Usar Tanzu Kubernetes Grid en Supervisor con Plano de control de IaaS de vSphere.

Utilizar la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*

Además de esta guía de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*, la documentación de vSphere IaaS control plane incluye otras guías. Asegúrese de familiarizarse con la jerarquía de la documentación de vSphere IaaS control plane, ya que algunas de las guías sirven como requisitos previos para los *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Esta ilustración describe cómo puede utilizar el conjunto de documentación de vSphere IaaS control plane y qué información puede encontrar en cada guía.

Figura 1-1. Mapa de documentación de vSphere IaaS control plane



Información actualizada

Esta documentación sobre *Servicios y cargas de trabajo del plano de control de IaaS de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Revisión	Descripción
25 de junio de 2024	Actualizaciones y mejoras generales para la versión vSphere 8.0 Update 3, incluidas las siguientes funciones: ■ Implementar servicios de supervisor en un entorno aislado. Consulte Capítulo 10 Implementar servicios de supervisor en un entorno aislado mediante la extracción de imágenes de un proxy. ■ Configurar parámetros de red y de equilibrador de carga para un espacio de nombres. Consulte Configurar parámetros de red y de equilibrador de carga para un espacio de nombres. ■ Admitir el operador de máquina virtual v1alpha2. Consulte Capítulo 6 Implementar y administrar máquinas virtuales en vSphere IaaS control plane. ■ Capacidad para utilizar `kubectl get virtualmachineclass` a fin de enumerar las clases de máquinas virtuales de un espacio de nombres de Supervisor específico. Antes, las clases de máquinas virtuales eran un recurso del ámbito del clúster, y era difícil determinar qué clases de máquinas virtuales estaban asignadas en un espacio de nombres específico. Consulte Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere IaaS control plane.
29 de abril de 2024	Se agregó una nota sobre las imágenes OVA disponibles que se pueden descargar de Imágenes recomendadas. Consulte Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere IaaS control plane.
1 de abril de 2024	Se actualizó Implementar una máquina virtual con vGPU y otros dispositivos PCI en vSphere IaaS control plane para incluir información sobre los parámetros avanzados utilizados con NVIDIA GRID vGPU.
29 de febrero de 2024	Se actualizó el contenido para editar una clase de máquina virtual para reflejar los cambios en el producto. Consulte Editar una clase de máquina virtual mediante vSphere Client.
11 de diciembre de 2023	Se agregó una declaración sobre las limitaciones de los volúmenes RWX respaldados por el servicio de archivos de vSAN. Consulte Usar el servicio de archivos de vSAN para crear volúmenes ReadWriteMany en vSphere IaaS control plane.
7 de noviembre de 2023	Se actualizó Usar el servicio de archivos de vSAN para crear volúmenes ReadWriteMany en vSphere IaaS control plane para aclarar que los volúmenes de archivos solo son compatibles con cargas de trabajo de clústeres de Tanzu Kubernetes Grid.
29 de septiembre de 2023	■ Se agregó nueva información de compatibilidad de plataforma sobre servicios de supervisor. Consulte Capítulo 4 Administrar servicios de supervisor con vSphere IaaS control plane. ■ Actualizaciones menores.

Revisión	Descripción
21 de septiembre de 2023	■ Se agregó nuevo contenido sobre el uso de los comandos de la CLI del centro de datos (DCLI) para asociar bibliotecas de contenido con un espacio de nombres o Supervisor. Consulte Agregar y administrar bibliotecas de contenido de máquina virtual en vSphere IaaS control plane. ■ Se agregó un tema sobre la publicación de nuevas imágenes de máquina virtual en una biblioteca de contenido en la que se puede escribir asociada con un espacio de nombres. Consulte Administrar y publicar imágenes de la biblioteca de contenido en vSphere IaaS control plane. ■ Se agregó nuevo contenido sobre el uso de los comandos de DCLI para crear y administrar las clases de máquinas virtuales. Consulte Crear y administrar clases de máquina virtual mediante la CLI del centro de datos.
14 de julio de 2023	■ Se mejoró la descripción de cómo se consumen los servicios de supervisor. Consulte Capítulo 4 Administrar servicios de supervisor con vSphere IaaS control plane. ■ Se agregó un requisito para anular la configuración de red de carga de trabajo de nivel 0 en Crear y configurar un espacio de nombres de vSphere en el Supervisor.
30 de junio de 2023	Se agregó el tema Quitar un espacio de nombres de vSphere de Supervisor.
21 de junio de 2023	Se aclaró la afirmación de que no se pueden expandir volúmenes creados como parte de StatefulSet cuando se utiliza la definición de StatefulSet. Consulte Expansión de volumen en vSphere IaaS control plane.
16 de mayo de 2023	Se agregó una nota que indica que, a partir de la versión vSphere 8 Update 1, servicios de supervisor están disponibles en Supervisores implementados con ambos tipos de redes, NSX o VDS. Consulte Capítulo 4 Administrar servicios de supervisor con vSphere IaaS control plane.
15 de mayo de 2023	Revisiones menores.
11 de mayo de 2023	■ Se agregó la tabla de compatibilidad de carga de trabajo a Capítulo 2 Flujos de trabajo para servicios y cargas de trabajo de vSphere IaaS control plane. ■ Se agregó una nota sobre una URL a la consola web de la máquina virtual que caduca en dos minutos si no se utiliza. Consulte Solucionar problemas de máquinas virtuales mediante la consola web de máquina virtual de vSphere. ■ Se agregó una ilustración que muestra la jerarquía de la documentación de vSphere IaaS control plane. Consulte Utilizar la documentación de Servicios y cargas de trabajo del plano de control de IaaS de vSphere.
9 de mayo de 2023	■ Se agregó la siguiente información: los volúmenes ReadWriteMany con una copia de seguridad creada por el servicio de archivos de vSAN no admiten la expansión de volúmenes. Consulte Expansión de volumen en vSphere IaaS control plane. ■ Se agregó información conceptual sobre pods de vSphere a Capítulo 7 Implementar cargas de trabajo en pods de vSphere.
5 de mayo de 2023	■ Se actualizó el capítulo Capítulo 9 Instalar y configurar Harbor y Contour en vSphere IaaS control plane. ■ Se agregó información que indica que los pods de vSphere solo se admiten con la pila de redes NSX. ■ Se agregó un ejemplo de implementación de pod de vSphere. Consulte Implementación de cargas de trabajo de pod de vSphere en vSphere IaaS control plane.

Revisión	Descripción
26 de abril de 2023	Se agregó el capítulo Capítulo 3 Configurar y administrar los espacios de nombres de vSphere.
18 de abril de 2023	■ Se agregó un tema sobre la implementación de máquinas virtuales con propiedades de OVF configurables. Consulte Implementar máquinas virtuales con propiedades OVF configurables en vSphere IaaS control plane. ■ Se agregó información sobre la consola web de máquina virtual de vSphere que los ingenieros de desarrollo y operaciones pueden utilizar para acceder directamente a una máquina virtual y a su sistema operativo invitado para solucionar problemas. Consulte Solucionar problemas de máquinas virtuales mediante la consola web de máquina virtual de vSphere.

Flujos de trabajo para servicios y cargas de trabajo de vSphere IaaS control plane

2

Estos flujos de trabajo asumen que ya ha habilitado vSphere IaaS control plane, ha configurado un Supervisor y ya está listo para crear espacios de nombres de vSphere y utilizarlos para cargas de trabajo.

Funciones de usuario

Por lo general, la interacción con el Supervisor y la ejecución de cargas de trabajo implica dos funciones: administrador de vSphere e ingeniero de desarrollo y operaciones. Los flujos de trabajo de las funciones de administrador de vSphere y de ingeniero de desarrollo y operaciones son distintos y se determinan según el área específica de conocimientos que estas requieren.

Administrador de vSphere

Como administrador de vSphere, por lo general, se utiliza vSphere Client para configurar un Supervisor y espacios de nombres en los que los ingenieros de desarrollo y operaciones puedan implementar cargas de trabajo de Kubernetes.

Si no creó su Supervisor y necesita obtener información sobre cómo hacerlo, consulte Instalar y configurar el plano de control de IaaS de vSphere.

Ingeniero de desarrollo y operaciones

En un Supervisor, una función de ingeniero de desarrollo y operaciones puede combinar actividades que normalmente realizan los desarrolladores de Kubernetes, los propietarios de aplicaciones y los administradores de Kubernetes. Como ingeniero de desarrollo y operaciones, puede utilizar comandos kubectl. Puede implementar y ejecutar pods de vSphere, máquinas virtuales y otras cargas de trabajo en espacios de nombres de Supervisor que el administrador de vSphere cree para usted. También puede crear espacios de nombres de autoservicio.

Debido a que esta guía de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere* no cubre las tareas que realiza el ingeniero de desarrollo y operaciones en un clúster de Tanzu Kubernetes Grid, para obtener información sobre estas tareas, consulte Usar Tanzu Kubernetes Grid en Supervisor con el plano de control de IaaS de vSphere .

Tipos de cargas de trabajo compatibles con un Supervisor

La compatibilidad de un Supervisor para diferentes tipos de cargas de trabajo depende de la configuración y las redes que utiliza el Supervisor.

Tipos de cargas de trabajo	Supervisor de una zona con redes VDS	Supervisor de una zona con redes NSX	Supervisor de tres zonas con redes VDS	Supervisor de tres zonas con redes NSX
Capítulo 7 Implementar cargas de trabajo en pods de vSphere	No	Sí	No	No
Capítulo 6 Implementar y administrar máquinas virtuales en vSphere IaaS control plane	Sí	Sí	Sí	Sí
Capítulo 4 Administrar servicios de supervisor con vSphere IaaS control plane	Sí	Sí	No	No
Clústeres de Tanzu Kubernetes Grid	Sí	Sí	Sí	Sí

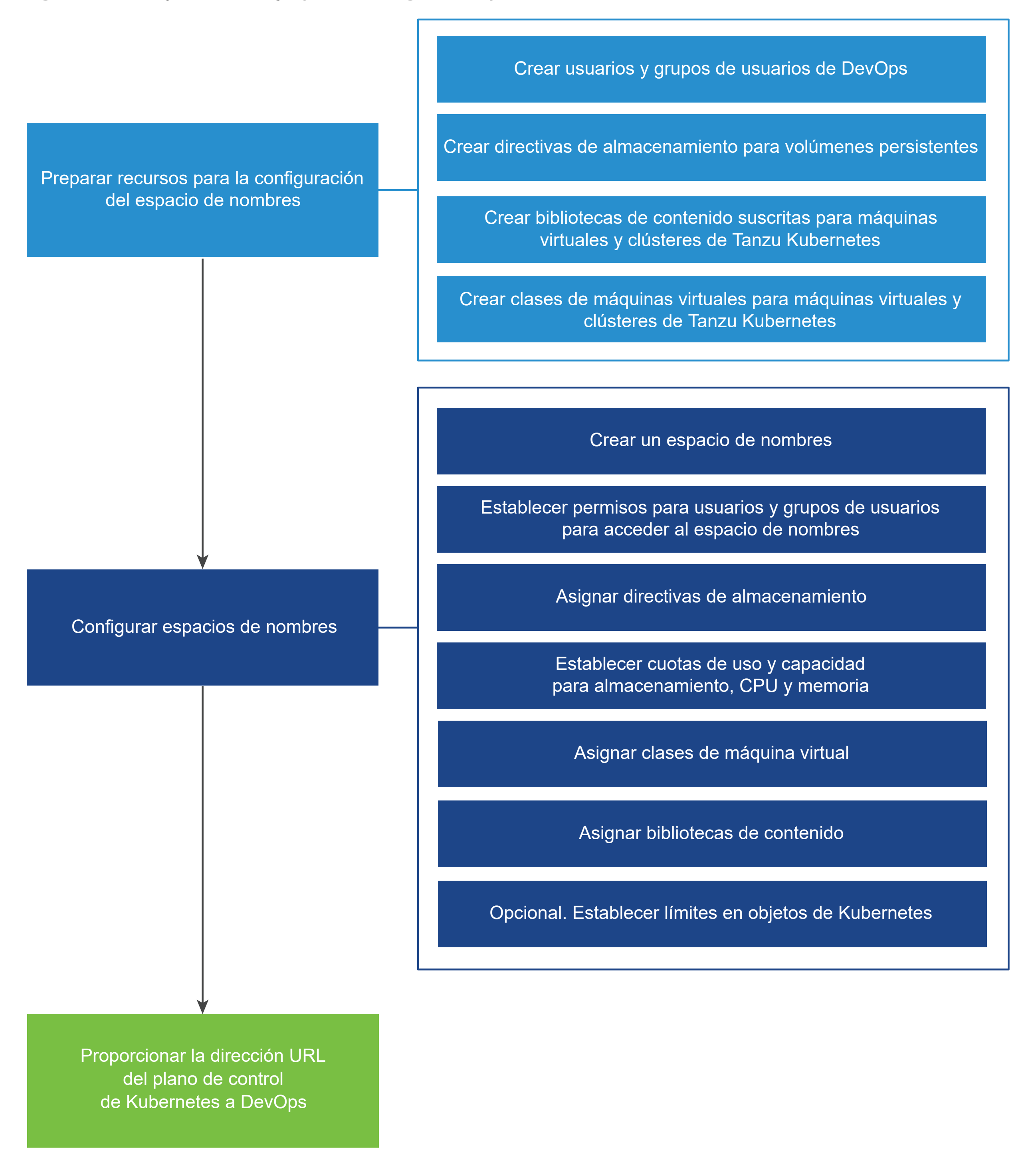
Flujo de trabajo para configurar espacios de nombres

Como administrador de vSphere, puede crear y administrar espacios de nombres de vSphere en un Supervisor. Clústeres de Tanzu Kubernetes Grid

Antes de crear un espacio de nombres, debe recopilar requisitos de recursos específicos de los ingenieros de desarrollo y operaciones sobre las aplicaciones y las cargas de trabajo que desean ejecutar. En función de estas especificaciones, puede configurar los recursos adecuados y asignarlos al espacio de nombres.

Para obtener más información, consulte Capítulo 3 Configurar y administrar los espacios de nombres de vSphere.

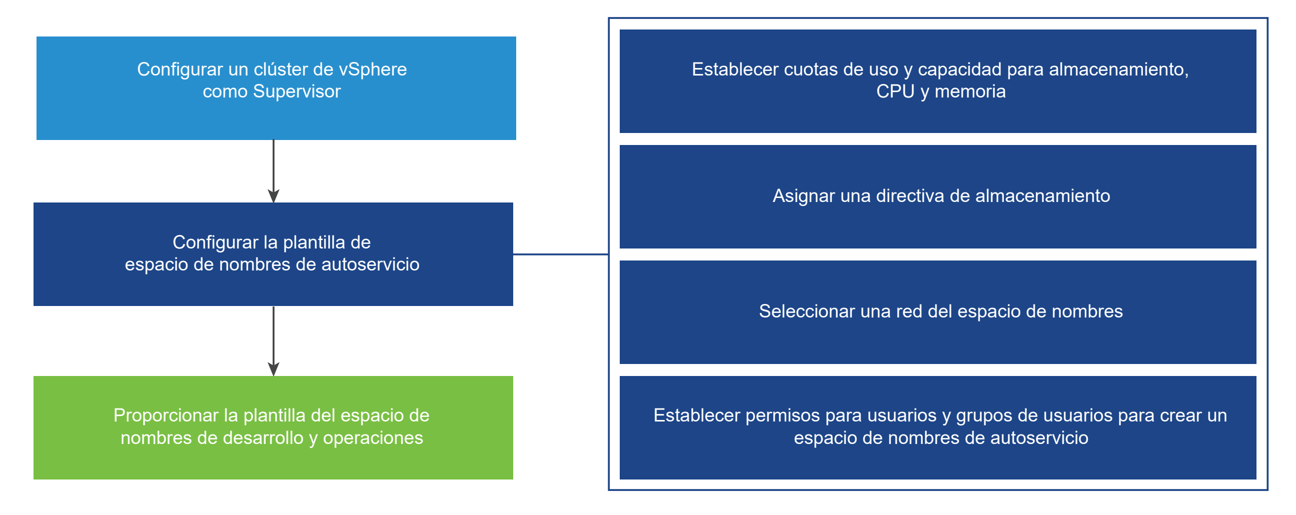
Figura 2-1. Flujo de trabajo para configurar espacios de nombres



Flujo de trabajo para configurar espacios de nombres de autoservicio

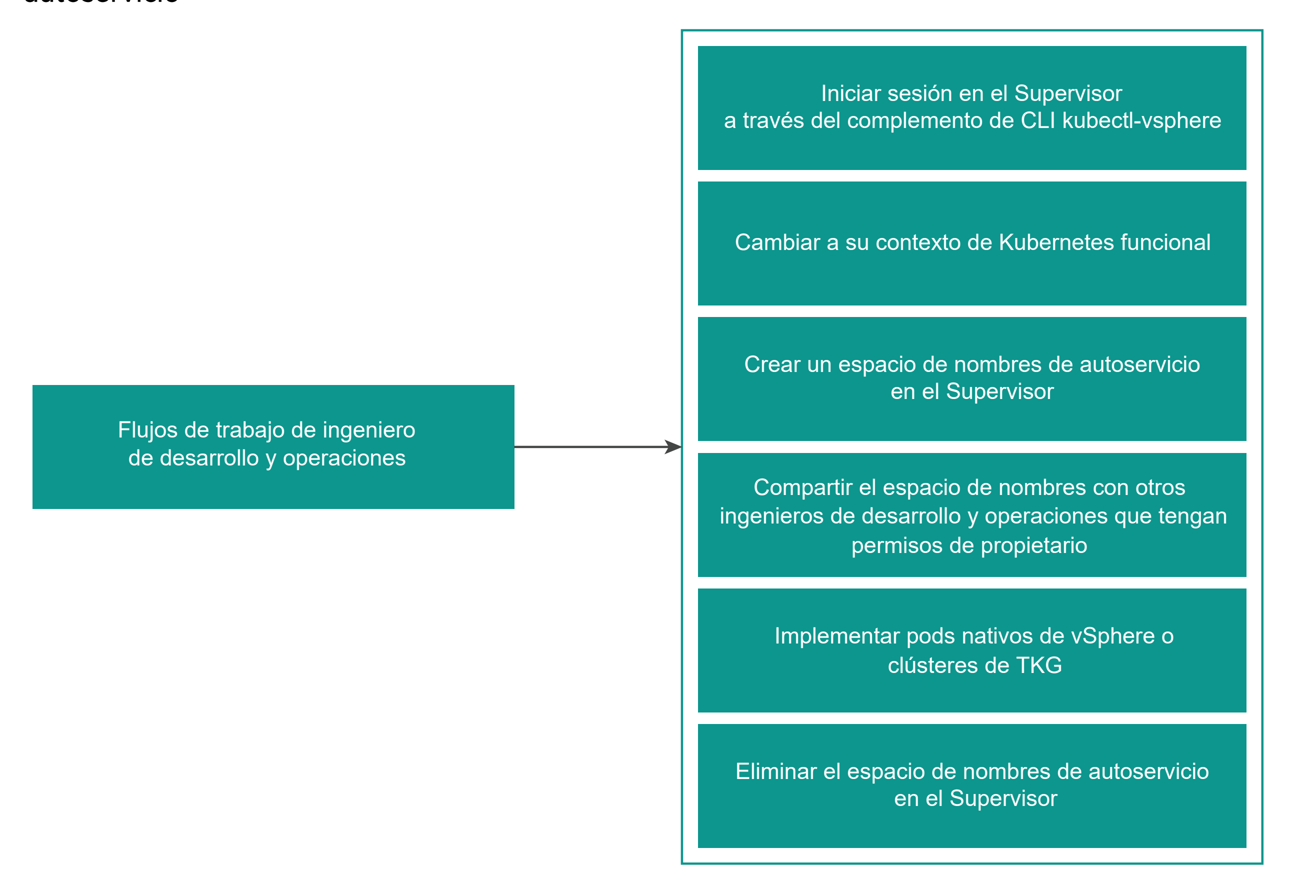
Como administrador de vSphere, puede crear un espacio de nombres de vSphere, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como plantilla. Para obtener más información, consulte Aprovisionar una plantilla de espacio de nombres de autoservicio en vSphere IaaS control plane.

Figura 2-2. Flujo de trabajo del administrador de vSphere para el espacio de nombres de autoservicio



Como ingeniero de Desarrollo y operaciones, puede crear un espacio de nombres de vSphere mediante autoservicio e implementar cargas de trabajo dentro de él. Puede compartirlo con otros ingenieros de Desarrollo y operaciones, o eliminarlo cuando ya no sea necesario.

Figura 2-3. Flujo de trabajo de desarrollo y operaciones para el espacio de nombres de autoservicio

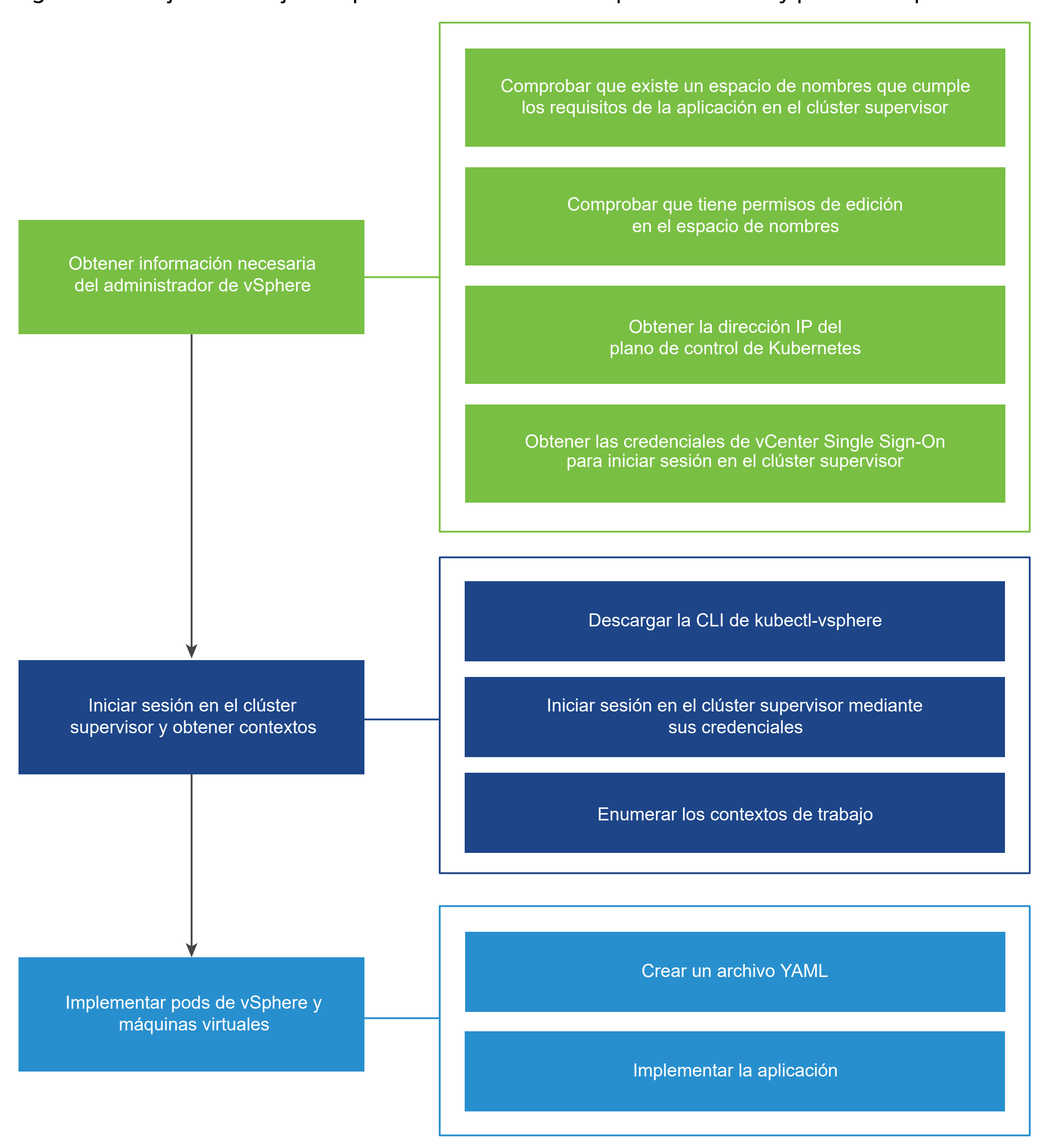


Flujo de trabajo para aprovisionamiento de pods de vSphere y máquinas virtuales

Como ingeniero de desarrollo y operaciones, puede implementar pods de vSphere y máquinas virtuales dentro de los límites de recursos de un espacio de nombres que se ejecuta en un Supervisor.

Para obtener más información, consulte Capítulo 7 Implementar cargas de trabajo en pods de vSphere y Capítulo 6 Implementar y administrar máquinas virtuales en vSphere IaaS control plane.

Figura 2-4. Flujo de trabajo de aprovisionamiento de máquinas virtuales y pods de vSphere



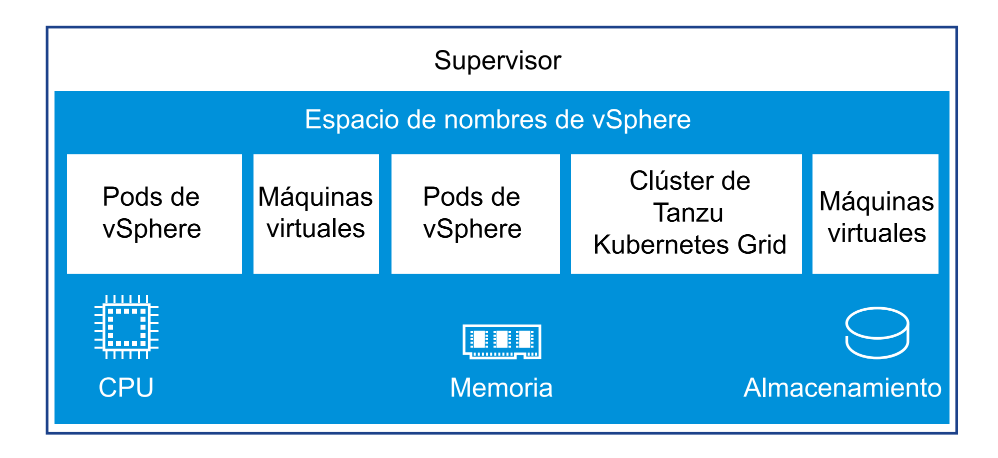
Configurar y administrar los espacios de nombres de vSphere

3

Las cargas de trabajo de vSphere IaaS control plane, incluidos los pods de vSphere, las máquinas virtuales y los clústeres de Tanzu Kubernetes, se implementan en un espacio de nombres de vSphere. Un administrador de vSphere define el espacio de nombres en un Supervisor y lo configura con cuota de recursos y permisos de usuario. En función de las necesidades de desarrollo y operaciones y las cargas de trabajo que planea ejecutar, el administrador de vSphere también puede asignar directivas de almacenamiento, clases de máquina virtual y bibliotecas de contenido para obtener las imágenes de máquina virtual.

Cuando se crea inicialmente, el espacio de nombres tiene recursos ilimitados dentro del Supervisor. Como administrador de vSphere, puede establecer límites para la CPU, la memoria y el almacenamiento, así como la cantidad de objetos de Kubernetes que se pueden ejecutar en el espacio de nombres. Las limitaciones de almacenamiento se representan como cuotas de almacenamiento en Kubernetes. Se crea un grupo de recursos en vSphere por cada espacio de nombres en el Supervisor

En un Supervisor activado en las Zonas de vSphere, se crea un grupo de recursos de espacio de nombres en cada clúster de vSphere que se asigna a una zona. Los recursos utilizados por el espacio de nombres en un Supervisor de tres zonas se toman de los tres clústeres de vSphere subyacentes en partes iguales. Por ejemplo, si dedica 300 MHz de CPU, se toman 100 MHz de cada clúster de vSphere.



Para otorgar acceso a los espacios de nombres al ingeniero de desarrollo y operaciones, el administrador de vSphere asigna permisos a los usuarios o a los grupos de usuarios disponibles en un origen de identidad que esté asociado con vCenter Single Sign-On o que provenga de un proveedor de ODIC que esté registrado en el Supervisor. Para obtener más información, consulte Administración de identidad y acceso del plano de control de vSphere IaaS.

Después de crear un espacio de nombres y configurarlo con límites de recursos y objetos, así como con permisos y directivas de almacenamiento, como ingeniero de desarrollo y operaciones, puede acceder al espacio de nombres para ejecutar las siguientes cargas de trabajo:

- Para obtener información sobre la ejecución de servicios de supervisor, consulte Capítulo 4 Administrar servicios de supervisor con vSphere IaaS control plane.
- Para obtener información sobre la ejecución de pods de vSphere, consulte Capítulo 7 Implementar cargas de trabajo en pods de vSphere.
- Para obtener información sobre la implementación de máquinas virtuales, consulte Capítulo 6 Implementar y administrar máquinas virtuales en vSphere IaaS control plane.

Nota Esta guía de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere* no incluye información sobre la ejecución de cargas de trabajo en un clúster de Tanzu Kubernetes Grid. Para obtener información sobre cómo trabajar con clústeres de Tanzu Kubernetes Grid, consulte Usar Tanzu Kubernetes Grid en Supervisor con Plano de control de IaaS de vSphere.

Lea los siguientes temas a continuación:

- Crear y configurar un espacio de nombres de vSphere en el Supervisor
- Quitar un espacio de nombres de vSphere de Supervisor
- Establecer límites de recursos en un espacio de nombres de vSphere
- Configurar limitaciones de objetos en un espacio de nombres de vSphere
- Supervisar y administrar recursos en un espacio de nombres de vSphere
- Aprovisionar una plantilla de espacio de nombres de autoservicio en vSphere IaaS control plane
- Cambiar la configuración de almacenamiento en un espacio de nombres vSphere
- Agregar directivas de seguridad a un espacio de nombres de vSphere de NSX
- Configurar parámetros de red y de equilibrador de carga para un espacio de nombres

Crear y configurar un espacio de nombres de vSphere en el Supervisor

Consulte cómo crear y configurar un espacio de nombres de vSphere en el Supervisor. Como administrador de vSphere, después de crear un espacio de nombres de vSphere, establezca límites de recursos en el espacio de nombres y los permisos para que los ingenieros de

desarrollo y operaciones puedan acceder a él. Debe proporcionar a los ingenieros de desarrollo y operaciones la dirección URL del plano de control de Kubernetes donde pueden ejecutar cargas de trabajo en los espacios de nombres para los que tienen permisos.

Los espacios de nombres de Supervisores que se configuran con la pila de redes de VDS y los espacios de nombres de los clústeres configurados con NSX tienen diferentes capacidades y configuración de redes. Los espacios de nombres que se configuran en Supervisores implementados en tres zonas de vSphere también admiten diferentes conjuntos de capacidades que los espacios de nombres en Supervisores con una sola zona.

- Supervisor de una zona configurado con NSX. Los espacios de nombres de vSphere en estos Supervisores admiten pods de vSphere, máquinas virtuales, clústeres de Tanzu Kubernetes Grid y servicios de supervisor. NSX proporciona la compatibilidad con redes de cargas de trabajo para estos espacios de nombres de vSphere.
- Supervisor de tres zonas con NSX. Los espacios de nombres de vSphere en un Supervisor de tres zonas configurado con NSX solo admiten máquinas virtuales y clústeres de Tanzu Kubernetes Grid. No admiten pods de vSphere ni servicios de supervisor.
- Supervisor de una zona configurado con VDS. Los espacios de nombres de vSphere en Supervisores de una zona con VDS admiten Tanzu Kubernetes Grid, máquinas virtuales y servicios de supervisor. No admiten otros pods de vSphere aparte de los que implementan los servicios de supervisor para su propio uso.
- Supervisor de tres zonas con VDS. Los espacios de nombres de vSphere que ejecutan un Supervisor de tres zonas con VDS solo admiten máquinas virtuales y clústeres de Tanzu Kubernetes Grid. No admiten pods de vSphere ni servicios de supervisor.

Si desea obtener más información, consulte Requisitos para habilitar un supervisor de tres zonas con el equilibrador de carga de HA Proxy y Requisitos para habilitar un supervisor de clúster único con redes de VDS y el equilibrador de carga de HA Proxy en *Planificación y conceptos del plano de control de IaaS de vSphere*.

También puede establecer límites de recursos para el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como una plantilla. Como resultado, los ingenieros de desarrollo y operaciones pueden crear un espacio de nombres de supervisor de autoservicio e implementar cargas de trabajo dentro de él. Para obtener más información, consulte Aprovisionar una plantilla de espacio de nombres de autoservicio en vSphere IaaS control plane.

Si utiliza NSX para sus Supervisores, tiene la opción de anular la configuración de red en el nivel del espacio de nombres de vSphere. Tenga en cuenta las siguientes consideraciones si selecciona esa opción:

Tabla 3-1. Consideraciones sobre la planificación de la red de espacio de nombres de vSphere

Consideración	Descripción
Instalación de NSX	Para anular la configuración de red del Supervisor para un espacio de nombres de vSphere en particular, NSX debe incluir un clúster de Edge dedicado para puertas de enlace de nivel 0 (enrutadores) y otro clúster de Edge dedicado para puertas de enlace de nivel 1. Consulte las instrucciones de instalación de NSX proporcionadas en la guía *Instalar y configurar el plano de control de IaaS de vSphere*.
Se requiere IPAM	Si anula la configuración de red del Supervisor para un espacio de nombres de vSphere en particular, la nueva red del espacio de nombres de vSphere debe especificar las subredes de Entrada, Salida y Red de espacio de nombres que sean únicas en el Supervisor y en cualquier otra red del espacio de nombres de vSphere. Tendrá que administrar la asignación de direcciones IP según corresponda.
Enrutamiento del Supervisor	El Supervisor debe poder enrutar directamente a los nodos del clúster de TKG y a las subredes de entrada. Al seleccionar una puerta de enlace de nivel 0 para el espacio de nombres de vSphere, existen dos opciones para configurar el enrutamiento que se requiere: ■ Utilizar una puerta de enlace de enrutamiento y reenvío virtual (Virtual Routing and Forwarding, VRF) para heredar la configuración de la puerta de enlace de nivel 0 del Supervisor ■ Utilizar el protocolo de puerta de enlace de borde (Border Gateway Protocol, BGP) para configurar rutas entre la puerta de enlace de nivel 0 del Supervisor y la puerta de enlace de nivel 0 dedicada Consulte la documentación de las puertas de enlace de nivel 0 de NSX para conocer más detalles sobre estas opciones.

Requisitos previos

- Implemente un Supervisor.
- Cree usuarios y grupos para desarrolladores e ingenieros de desarrollo y operaciones, quienes necesitarán acceso al espacio de nombres de vSphere. Cree los usuarios o los grupos en orígenes de identidad que estén conectados a vCenter Single Sign-On o en un proveedor de OIDC configurado con el Supervisor.
- Cree directivas de almacenamiento para el almacenamiento persistente. Si el espacio de nombres se encuentra en un Supervisor de tres zonas, utilice directivas con reconocimiento de topología. No se pueden asignar directivas de almacenamiento sin reconocimiento de topología al espacio de nombres de tres zonas.
- Cree clases de máquina virtual y bibliotecas de contenido para máquinas virtuales independientes.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione la pestaña **Espacios de nombres**.

3 Haga clic en **Crear espacio de nombres**.

4 Seleccione el Supervisor donde quiere ubicar el espacio de nombres de vSphere.

5 Introduzca un nombre para el espacio de nombres.

El nombre debe tener un formato compatible con DNS.

6 En el menú desplegable **Red**, seleccione una red de cargas de trabajo para el espacio de nombres de vSphere.

Nota Este paso solo está disponible si se crea el espacio de nombres en un clúster que se haya configurado con la pila de redes de vSphere.

7 Si configuró la pila de redes de NSX para el Supervisor, puede seleccionar **Anular configuración de red de clúster** para anular la configuración de red del Supervisor y configurar los ajustes de red para el espacio de nombres.

Configure los siguientes ajustes de red para el espacio de nombres:

Opción	Descripción
Puerta de enlace de nivel 0	Seleccione la puerta de enlace de nivel 0 que se asociará con la puerta de enlace de nivel 1 del espacio de nombres. Al seleccionar una puerta de enlace de nivel 0, se anula la puerta de enlace de nivel 0 que configuró al habilitar el clúster, por lo que debe volver a configurar los rangos de CIDR. **Nota** El Supervisor debe poder enrutar directamente a los nodos del clúster de TKG y a las subredes de entrada. ■ Si selecciona una puerta de enlace VRF vinculada a la puerta de enlace de nivel 0, la red y las subredes se configuran automáticamente. ■ Si seleccionó el modo NAT, debe configurar los CIDR de subred, entrada y salida. ■ Si anula la selección del modo NAT, solo debe configurar la subred y los CIDR de entrada. **Nota** Una vez que seleccione una puerta de enlace de nivel 0, no podrá cambiarla.
Modo NAT	El modo NAT está seleccionado de forma predeterminada. Si anula la selección de esta opción, todas las cargas de trabajo, como las direcciones IP del nodo de pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes Grid, son accesibles directamente desde fuera de la puerta de enlace de nivel 0 y no es necesario configurar los CIDR de salida. **Nota** Una vez habilitado el modo de espacio de nombres, no se pueden hacer cambios.
Tamaño del equilibrador de carga	Seleccione el tamaño de la instancia del equilibrador de carga en la puerta de enlace de nivel 1 para el espacio de nombres.

Opción	Descripción
Red de espacio de nombres	Introduzca uno o varios CIDR de IP para crear subredes/segmentos y asignar direcciones IP para cargas de trabajo conectadas a espacios de nombres. **Nota** Introduzca el rango de CIDR si no lo configuró para el clúster. Puede configurar CIDR adicionales después de crear el espacio de nombres editando la configuración de red del espacio de nombres.
Prefijo de subred de espacio de nombres	Introduzca el prefijo de subred que especifica el tamaño de la subred reservada para los segmentos de espacios de nombres. El valor predeterminado es 28. **Nota** Una vez que especifique el prefijo de subred, no podrá cambiarlo.
Ingreso	Introduzca una anotación CIDR que determine el rango de IP de entrada para las direcciones IP virtuales publicadas por el servicio de equilibrador de carga para clústeres de pods de vSphere o Tanzu Kubernetes Grid. Puede configurar CIDR adicionales después de crear el espacio de nombres editando la configuración de red del espacio de nombres.
Egreso	Introduzca una anotación CIDR que determine el rango de IP de egreso para las direcciones IP SNAT. Puede configurar CIDR adicionales después de crear el espacio de nombres editando la configuración de red del espacio de nombres.

8 Introduzca una descripción y haga clic en **Crear**.

El espacio de nombres se crea en el Supervisor.

9 Establezca permisos para los usuarios que puedan acceder al espacio de nombres.

Como administrador de vSphere, establezca permisos en un espacio de nombres de vSphere para desarrolladores e ingenieros de desarrollo y operaciones que necesitan acceder al espacio de nombres. Una cuenta de usuario puede tener acceso a varios espacios de nombres a la vez. Los usuarios que pertenecen a los grupos de administradores pueden acceder a todos los espacios de nombres del Supervisor.

a En el panel **Permisos**, seleccione **Agregar permisos**.

b Seleccione un origen de identidad, un usuario o un grupo, y una función, y haga clic en **Aceptar**.

Función	Descripción
Puede ver	Acceso de solo lectura para el usuario o el grupo. El usuario o el grupo pueden iniciar sesión en el plano de control del Supervisor y crear una lista con las cargas de trabajo que se ejecutan en el espacio de nombres de vSphere, como los pods de vSphere y los clústeres de Tanzu Kubernetes Grid, y las máquinas virtuales.
Puede editar	El usuario o el grupo pueden crear, leer, actualizar y eliminar pods de vSphere, clústeres de Tanzu Kubernetes Grid y máquinas virtuales. Los usuarios que forman parte del grupo Administradores tienen permisos de edición en todos los espacios de nombres del Supervisor.
Propietario	Las cuentas de usuario con permisos de propietario pueden hacer lo siguiente: ■ Implemente y administre cargas de trabajo en el espacio de nombres. ■ Comparta el espacio de nombres con otros usuarios o grupos. ■ Crear y eliminar espacios de nombres de vSphere adicionales mediante kubectl. Cuando usuarios con el permiso de propietario comparten el espacio de nombres, pueden asignar permisos de vista, edición o propietario a otros usuarios o grupos. **Nota** La función de propietario es compatible con los usuarios disponibles en el origen de identidad de vCenter Single Sign-On. No se puede usar la función de propietario con un usuario o grupo que provenga de un proveedor de identidad externo.

Cuando asigna un usuario o grupo a las funciones **`Puede ver`** o **`Puede editar`**, el sistema crea un objeto RoleBinding y lo asigna a un objeto ClusterRole. Por ejemplo, un usuario o grupo asignados a la función **`Puede editar`** se asignan al objeto `edit` ClusterRole de Kubernetes mediante un objeto RoleBinding. Con la función `edit`, los usuarios pueden aprovisionar y operar clústeres. Puede ver esta asignación mediante el comando `kubectl get rolebinding` desde el espacio de nombres de vSphere de destino.

```
kubectl get rolebinding -n tkg2-cluster-namespace
NAME
ROLE                                AGE
```

```
wcp:tkg-cluster-namespace:group:vsphere.local:administrators   ClusterRole/
edit             33d
wcp:tkg-cluster-namespace:user:vsphere.local:administrator     ClusterRole/
edit             33d
```

Cuando se asigna un usuario o grupo a la función de propietario, el sistema crea un objeto ClusterRoleBinding y lo asigna a un objeto ClusterRole que permite al usuario o grupo crear y eliminar espacios de nombres de vSphere mediante kubectl. Para ver esta asignación, puede utilizar SSH con un nodo de plano de control del Supervisor.

10 Asigne el almacenamiento al espacio de nombres.

Las directivas de almacenamiento que se asignan al espacio de nombres ponen el almacenamiento persistente a disposición del equipo de desarrollo y operaciones.

a En el panel **Almacenamiento**, seleccione **Agregar almacenamiento**.

b Seleccione una directiva de almacenamiento para controlar la ubicación de los almacenes de datos de los volúmenes persistentes y haga clic en **Aceptar**.

Después de asignar la directiva de almacenamiento, vSphere IaaS control plane crea una clase de almacenamiento de Kubernetes que coincide en el espacio de nombres de vSphere. Si utiliza Tanzu Kubernetes Grid, la clase de almacenamiento se replica automáticamente desde el espacio de nombres en el clúster de Tanzu Kubernetes Grid. Si asigna varias directivas de almacenamiento al espacio de nombres, se crea una clase de almacenamiento independiente para cada directiva de almacenamiento.

11 En el panel Capacidad y uso, seleccione **Editar límites** y configure las limitaciones de recursos en el espacio de nombres.

Opción	Descripción
CPU	La cantidad de recursos de CPU que se reservarán para el espacio de nombres.
Memoria	La cantidad de memoria que se reservará para el espacio de nombres.
Almacenamiento	La cantidad total de espacio de almacenamiento que se reservará para el espacio de nombres.
Límites de directivas de almacenamiento	Establezca la cantidad de almacenamiento dedicado individualmente a cada una de las directivas de almacenamiento que asoció al espacio de nombres.

Se crea un grupo de recursos para el espacio de nombres en vCenter Server. La limitación de almacenamiento determina la cantidad total de almacenamiento disponible para el espacio de nombres, mientras que las directivas de almacenamiento determinan la colocación de los volúmenes persistentes para los pods de vSphere en las clases de almacenamiento asociadas.

12 Configure el servicio de máquina virtual para las máquinas virtuales independientes.

Para obtener información, consulte Capítulo 6 Implementar y administrar máquinas virtuales en vSphere IaaS control plane.

Pasos siguientes

Comparta la URL del plano de control de Kubernetes con los ingenieros de desarrollo y operaciones, así como el nombre de usuario que pueden utilizar para iniciar sesión en Supervisor a través de Herramientas de la CLI de Kubernetes para vSphere. Puede conceder acceso a más de un espacio de nombres a un ingeniero de desarrollo y operaciones. Consulte Conectarse a clústeres del plano de control de vSphere IaaS.

Nota Esta guía de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere* no incluye información sobre la ejecución de cargas de trabajo en un clúster de Tanzu Kubernetes Grid. Para obtener información sobre cómo trabajar con clústeres de Tanzu Kubernetes Grid, consulte Usar Tanzu Kubernetes Grid en Supervisor con Plano de control de IaaS de vSphere.

Quitar un espacio de nombres de vSphere de Supervisor

Puede quitar un espacio de nombres de vSphere de Supervisor

Requisitos previos

- Elimine todas las cargas de trabajo implementadas, incluidas las máquinas virtuales, los pods de vSphere y los clústeres de TKG. Para obtener información sobre cómo eliminar un clúster de TKG, consulte Eliminar un clúster de TKG 2.0 con Kubectl o con la CLI de Tanzu.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Haga clic en la pestaña **Espacios de nombres**.

3 En la lista de espacios de nombres disponibles en el Supervisor, seleccione el espacio de nombres de vSphere que desea eliminar.

4 Haga clic en **Quitar**.

   El sistema elimina el espacio de nombres de vSphere. El proceso puede tardar un tiempo en completarse.

Establecer límites de recursos en un espacio de nombres de vSphere

Como administrador de vSphere, puede establecer límites de recursos y valores predeterminados de contenedor en un espacio de nombres de vSphere. Los ingenieros de desarrollo y operaciones pueden reemplazar posteriormente los valores predeterminados del contenedor en las especificaciones del pod, pero sin superar los límites de recursos totales

establecidos en el espacio de nombres por el administrador de vSphere. Las solicitudes de contenedor se traducen en reservas de recursos en pods.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración del espacio de nombres** en Supervisor.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione un espacio de nombres de vSphere, seleccione **Configurar** y haga clic en **Límites de recursos**.

3 Haga clic en **Editar**.

El impacto del establecimiento de límites de recursos para un espacio de nombres de vSphere en el que se aprovisionan clústeres de Tanzu Kubernetes Grid varía en función del tipo de clase de máquina virtual utilizada para los nodos del clúster. Asegúrese de estar al tanto de las diferencias entre el mejor esfuerzo y el garantizado antes de establecer los límites de recursos. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes en *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Opción	Descripción
CPU	Establezca un límite para el consumo de CPU en el espacio de nombres de vSphere.
Memoria	Establezca un límite para el consumo de memoria en el espacio de nombres de vSphere.
Almacenamiento	Establezca un límite para el consumo de almacenamiento en el espacio de nombres de vSphere por directiva de almacenamiento que se utilice.
Valores predeterminados del contenedor	Establezca los valores predeterminados para los límites de CPU, las solicitudes de CPU, las solicitudes de memoria y los límites de memoria para contenedores en el espacio de nombres de vSphere.

Configurar limitaciones de objetos en un espacio de nombres de vSphere

Es posible configurar limitaciones para los objetos que se ejecutan en el espacio de nombres de vSphere, como el número de implementaciones, trabajos, conjuntos de daemons y conjuntos con estado, entre otros. Las limitaciones que se configuran para un objeto dependen de los detalles de las aplicaciones y del modo en que desea que consuman los recursos dentro de un espacio de nombres de vSphere.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración del espacio de nombres** en Supervisor.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione el espacio de nombres de vSphere en el que desea aplicar las restricciones de objeto o contenedor.

3 Seleccione **Configurar** y, a continuación, **Límites de objetos**.

4 Haga clic en **Editar**.

Opción	Descripción
Pods de vSphere	La cantidad de pods de vSphere que pueden ejecutarse en el espacio de nombres de vSphere.
Implementaciones	La cantidad de implementaciones que pueden ejecutarse en el espacio de nombres de vSphere.
Trabajos	La cantidad de trabajos que pueden ejecutarse en el espacio de nombres de vSphere.
Conjuntos de daemons	La cantidad de conjuntos de daemons que pueden ejecutarse en el espacio de nombres de vSphere.
Conjuntos de réplicas	La cantidad de conjuntos de réplicas en el espacio de nombres de vSphere.
Controladoras de replicación	La cantidad de controladoras de replicación que pueden ejecutarse en el espacio de nombres de vSphere.
Conjuntos con estado	La cantidad de StatefulSets que pueden ejecutarse en el espacio de nombres de vSphere.
Mapas de configuración	La cantidad de ConfigMaps que pueden ejecutarse en el espacio de nombres de vSphere.
Secretos	La cantidad de secretos que pueden ejecutarse en el espacio de nombres de vSphere.
Notificaciones de volumen persistente	Las notificaciones de volumen persistente que pueden existir en el espacio de nombres de vSphere.
Servicios	Los servicios que pueden existir en el espacio de nombres de vSphere.

Supervisar y administrar recursos en un espacio de nombres de vSphere

Es posible supervisar y administrar diferentes aspectos de un espacio de nombres de vSphere, como el consumo de recursos para el espacio de nombres o la cantidad de objetos de Kubernetes diferentes que existen en un espacio de nombres y sus estados.

Requisitos previos

Crear y configurar un espacio de nombres de vSphere.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Desplácese hasta la vista **Menú > Hosts y clústeres**.

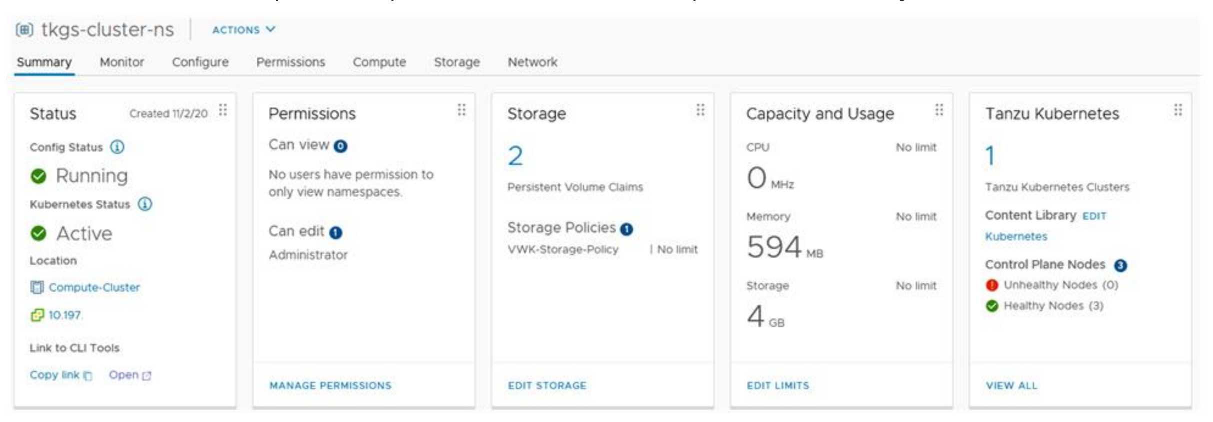
3 Seleccione el clúster de vCenter en el que ha habilitado **Administración de cargas de trabajo**.

4 Seleccione el grupo de recursos de **Espacios de nombres** y expanda su contenido.

   Los nodos del plano de control del Supervisor se encuentran en el grupo de recursos de Espacios de nombres. Además, cada espacio de nombres de vSphere que se crea para este Supervisor se encuentra en el grupo de recursos **Espacios de nombres**.

5 Seleccione el objeto del espacio de nombres de vSphere, que se representa como un icono de ventana.

   En la pestaña **Resumen**, verá las diferentes secciones de configuración del espacio de nombres de vSphere, incluidas **Estado**, **Permisos**, **Almacenamiento**, **Capacidad y uso** y **Tanzu Kubernetes**. En esta pantalla, puede administrar cualquiera de estos ajustes.



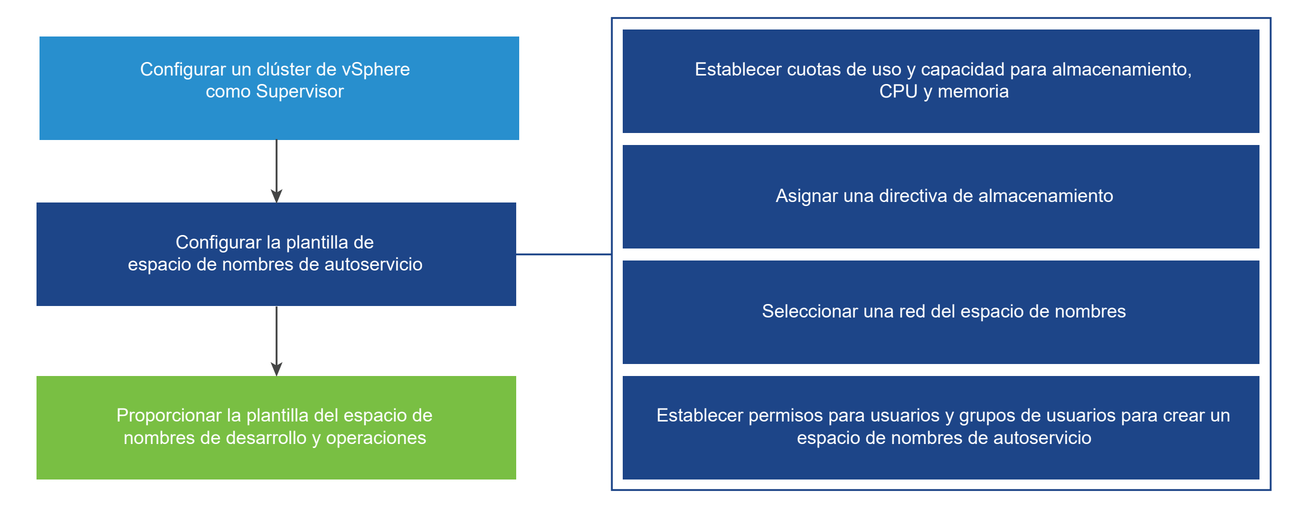
Aprovisionar una plantilla de espacio de nombres de autoservicio en vSphere IaaS control plane

Como administrador de vSphere, puede crear un espacio de nombres de supervisor, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y activar el servicio de espacio de nombres en un clúster como una plantilla. Como resultado, los ingenieros de desarrollo y operaciones pueden crear un espacio de nombres de supervisor de autoservicio e implementar cargas de trabajo dentro de él.

Flujo de trabajo de creación y configuración de espacios de nombres de autoservicio

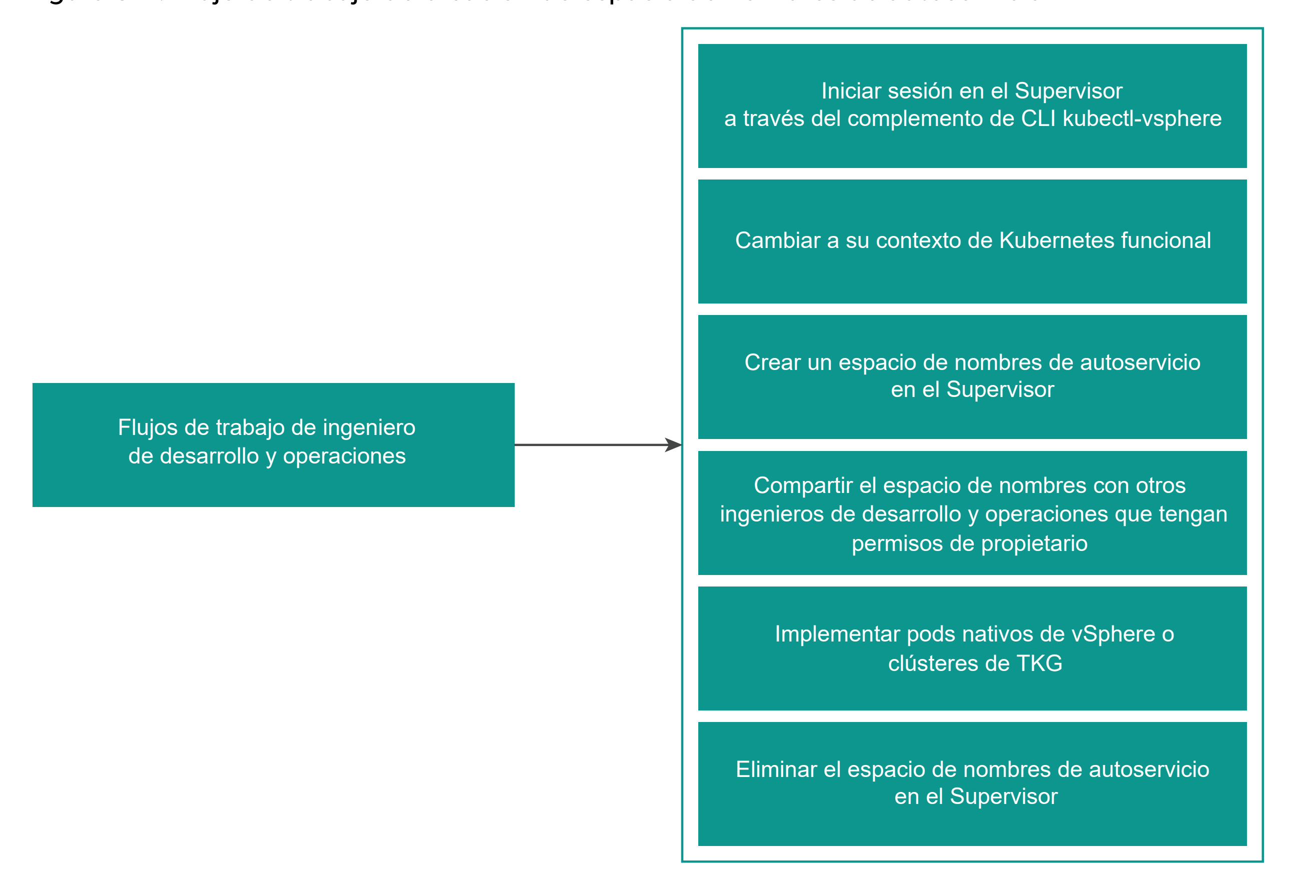
Como administrador de vSphere, puede crear un espacio de nombres de supervisor, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como plantilla.

Figura 3-1. Flujo de trabajo de aprovisionamiento de plantilla de espacio de nombres de autoservicio



Como ingeniero de Desarrollo y operaciones, puede crear un espacio de nombres de supervisor mediante autoservicio e implementar cargas de trabajo dentro de él. Puede compartirlo con otros ingenieros de Desarrollo y operaciones, o eliminarlo cuando ya no sea necesario. Para compartir el espacio de nombres con otros ingenieros de desarrollo y operaciones, póngase en contacto con el administrador de vSphere.

Figura 3-2. Flujo de trabajo de creación de espacio de nombres de autoservicio



Crear y configurar una plantilla de espacio de nombres de autoservicio

Como administrador de vSphere, puede crear y configurar un espacio de nombres de supervisor como una plantilla de espacio de nombres de autoservicio. A continuación, los ingenieros de desarrollo y operaciones pueden crear y eliminar espacios de nombres de supervisor mediante la línea de comandos de `kubectl`.

Requisitos previos

Configure un clúster con vSphere IaaS control plane.

Procedimiento

1 En vSphere Client, desplácese hasta Supervisor.

2 Haga clic en la pestaña **Configurar** y seleccione **General** en **Supervisor**.

3 Seleccione **Servicio de espacio de nombres**.

4 Active o desactive el conmutador **Estado** para habilitar la función.

   Aparecerá la página **Crear plantilla de espacio de nombres**.

5 En el panel **Configuración**, configure recursos para el espacio de nombres.

Opción	Descripción
CPU	La cantidad de recursos de CPU que se reservarán para el espacio de nombres.
Memoria	La cantidad de memoria que se reservará para el espacio de nombres.
Almacenamiento	La cantidad total de espacio de almacenamiento que se reservará para el espacio de nombres.
Directiva de almacenamiento	Las directivas de almacenamiento que se usarán con cargas de trabajo que requieren almacenamiento persistente.
Red	En el menú desplegable **Red**, seleccione una red para el espacio de nombres.
Clases de máquina virtual	Las clases de máquina virtual para implementar máquinas virtuales independientes.
Bibliotecas de contenido	Las bibliotecas de contenido con imágenes de máquina virtual que se usarán para las implementaciones de máquinas virtuales.

6 Haga clic en **Siguiente**.

7 En el panel **Permisos**, agregue ingenieros y grupos de desarrollo y operaciones para permitirles utilizar la plantilla con la que pueden crear espacios de nombres.

   Seleccione un origen de identidad y un usuario o un grupo, y haga clic en **Siguiente**.

8 En el panel **Revisar y confirmar**, se muestran las propiedades que configura.

Revise las propiedades y haga clic en **Listo**.

Resultados

Se configuró una plantilla de espacio de nombres y tiene estado Activo. Como administrador de vSphere, puede editar la plantilla. Los ingenieros de desarrollo y operaciones pueden utilizar la plantilla para crear espacios de nombres.

Desactivar un espacio de nombres de autoservicio

Como administrador de vSphere, puede desactivar un espacio de nombres de autoservicio en el clúster.

Cuando se desactiva una plantilla de espacio de nombres de autoservicio, los ingenieros de desarrollo y operaciones no pueden usar la plantilla para crear nuevos espacios de nombres en el clúster. Sí pueden eliminar los espacios de nombres que ya crearon.

Procedimiento

1 En vSphere Client, desplácese hasta Supervisor.

2 Haga clic en la pestaña **Configurar** y seleccione **General** en **Supervisor**.

3 En el panel **Servicio de espacio de nombres**, alterne el conmutador de **Estado** para desactivar la plantilla.

4 Para volver a activar la plantilla, alterne nuevamente el conmutador de **Estado**.

Puede crear otro espacio de nombres de autoservicio o utilizar el existente.

Crear un espacio de nombres de autoservicio

Como ingeniero de desarrollo y operaciones, puede crear un espacio de nombres de autoservicio y ejecutar cargas de trabajo en él. Una vez creado el espacio de nombres, puede compartirlo con otros ingenieros de desarrollo y operaciones o eliminarlo cuando ya no sea necesario.

Requisitos previos

- Compruebe que un administrador de vSphere haya creado y activado una plantilla de espacio de nombres de autoservicio en el clúster. Consulte Crear y configurar una plantilla de espacio de nombres de autoservicio .
- Compruebe que se haya agregado a la lista de permisos en la plantilla de espacio de nombres de autoservicio de forma individual o como miembro de un grupo.
- Obtenga la dirección IP del plano de control de Supervisor.

Procedimiento

1 Utilice complemento de vSphere para kubectl para autenticarse en Supervisor. Consulte Conexión con el supervisor como usuario de vCenter Single Sign-On.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al Supervisor.

```
kubectl config use-context SUPERVISOR-CLUSTER-IP
```

3 Cree un espacio de nombres de autoservicio en el clúster.

```
kubectl create namespace NAMESPACE NAME
```

Por ejemplo

```
kubectl create namespace test-ns
```

Nota Los permisos de propietario están disponibles para los ingenieros de desarrollo y operaciones después de habilitar vSphere IaaS control plane y actualizar el clúster. Si solo actualizó vCenter Server y no el clúster, los ingenieros de desarrollo y operaciones solo tendrán permisos de edición en los espacios de nombres.

El espacio de nombres que cree aparecerá en el clúster. Para compartir el espacio de nombres con otros ingenieros de desarrollo y operaciones, póngase en contacto con el administrador de vSphere.

Crear un espacio de nombres de autoservicio con anotaciones y etiquetas

Los ingenieros de desarrollo y operaciones pueden crear espacios de nombres de autoservicio con anotaciones y etiquetas mediante la línea de comandos kubectl.

Los ingenieros de desarrollo y operaciones pueden utilizar un manifiesto de YAML con anotaciones y etiquetas definidas por el usuario.

Procedimiento

1 Inicie sesión en el Supervisor.

`kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME`

2 Cree un archivo de manifiesto YAML de espacio de nombres con anotaciones y etiquetas.

`kubectl create -f ns-create.yaml`

Por ejemplo, cree el siguiente archivo `ns-create.yaml`:

```
apiVersion: v1
kind: Namespace
```

```
metadata:
  name: test-ns-yaml
  labels:
    my-label: "my-label-val-yaml"
  annotations:
    my-ann-yaml: "my-ann-val-yaml"
```

3 Aplique el manifiesto de YAML.

`kubectl create -f ns-create.yaml`

O

`kubectl apply -f ns-create.yaml`

4 Describa el espacio de nombres que creó para ver los cambios.

```
root@localhost [ /tmp ]# kubectl describe ns test-ns-yaml
Name:         test-ns-yaml
Labels:       my-label=my-label-val-yaml
              vSphereClusterID=domain-c50
Annotations:  my-ann-yaml: my-ann-val-yaml
              vmware-system-namespace-owner-count: 1
              vmware-system-resource-pool: resgroup-171
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v172
Status:       Active

Resource Quotas
 Name:             test-ns-yaml
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi

 Name:                                                                     test-ns-
yaml-storagequota
 Resource                                                                  Used  Hard
 --------                                                                  ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807

No LimitRange resource.
```

Actualizar un espacio de nombres de autoservicio mediante la anotación kubectl y la etiqueta kubectl

El ingeniero de desarrollo y operaciones puede actualizar o eliminar las anotaciones y etiquetas del espacio de nombres de autoservicio mediante los comandos `kubectl annotate` y `kubectl label`.

Requisitos previos

Compruebe que tiene permisos de propietario en el espacio de nombres que desea actualizar.

Procedimiento

1 Inicie sesión en el Supervisor.

`kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME`

2 Describa el espacio de nombres que desea actualizar.

```
root@localhost [ /tmp ]# kubectl describe ns testns
Name:         testns
Labels:       my-label=test-label-2
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-2
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                         testns-
storagequota
 Resource                                                                      Used  Hard
 --------                                                                      ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807
```

3 Actualice las anotaciones mediante el comando `kubectl annotate`.

Por ejemplo, `kubectl annotate --overwrite ns testns my-ann="test-ann-3"`

Para eliminar una anotación, ejecute el comando `kubectl annotate --overwrite ns testns my-ann-`

4 Actualice las etiquetas mediante el comando `kubectl label`.

Por ejemplo, `kubectl label --overwrite ns testns my-label="test-label-3"`

Para eliminar una etiqueta, ejecute el comando `kubectl label --overwrite ns testns my-label-`

5 Describa el espacio de nombres para ver las actualizaciones.

```
root@localhost [ /tmp ]# kubectl describe ns testns
Name:         testns
Labels:       my-label=test-label-3
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-3
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                          testns-
storagequota
 Resource                                                                       Used  Hard
 --------                                                                       ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807


No LimitRange resource.
```

Actualizar un espacio de nombres de autoservicio mediante kubectl edit

El ingeniero de desarrollo y operaciones puede actualizar los espacios de nombres de autoservicio mediante el comando `kubectl edit`.

Requisitos previos

Compruebe que tiene permisos de propietario en el espacio de nombres que desea actualizar.

Procedimiento

1 Inicie sesión en el Supervisor.

```
kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-
username VCENTER-SSO-USERNAME
```

2 Describa el espacio de nombres que desea actualizar.

```
kubectl describe ns testns-1
Name:         testns
```

```
Labels:       vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-2
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns-1
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                          testns-1-
storagequota
 Resource                                                                       Used  Hard
 --------                                                                       ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807
```

3 Edite el espacio de nombres mediante el comando `kubectl edit`.

Por ejemplo, `kubectl edit ns testns-1`

El comando `kubectl edit` abre el manifiesto del espacio de nombres en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR.

4 Actualice las etiquetas.

Por ejemplo, `my-label=test-label`

5 Actualice las anotaciones.

Por ejemplo, `my-ann: test-ann`

6 Describa el espacio de nombres para ver las actualizaciones.

```
root@localhost [ /tmp ]# kubectl describe ns testns-1
Name:         testns-1
Labels:       my-label=test-label
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann
              vmware-system-namespace-owner-count: 1
              vmware-system-resource-pool: resgroup-173
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v174
Status:       Active
```

```
Resource Quotas
 Name:              testns-1
 Resource           Used  Hard
 --------           ---   ---
 requests.storage   0     5000Mi


 Name:                                                                              testns-1-
storagequota
 Resource                                                                           Used  Hard
 --------                                                                           ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage   0
9223372036854775807


No LimitRange resource.
```

Eliminar un espacio de nombres de autoservicio

Como ingeniero de desarrollo y operaciones, puede eliminar un espacio de nombres de autoservicio que haya creado.

Requisitos previos

Compruebe si creó un espacio de nombres de autoservicio mediante el complemento de vSphere para kubectl.

Procedimiento

1 Utilice complemento de vSphere para kubectl para autenticarse en Supervisor. Consulte Conexión con el supervisor como usuario de vCenter Single Sign-On.

2 Elimine el espacio de nombres de autoservicio del clúster.

```
kubectl delete namespace NAMESPACE NAME
```

Por ejemplo:

```
kubectl delete namespace test-ns
```

Cambiar la configuración de almacenamiento en un espacio de nombres vSphere

Las directivas de almacenamiento asignadas a un espacio de nombres en un Supervisor hacen que el almacenamiento persistente esté disponible para el equipo de desarrollo y operaciones. Estas directivas de almacenamiento controlan cómo se colocan los volúmenes persistentes y los nodos del clúster de Tanzu Kubernetes dentro de los almacenes de datos de vSphere.
Por lo general, como administrador de vSphere, asigna las directivas de almacenamiento al configurar el espacio de nombres. Si necesita realizar cambios en las asignaciones de directivas de almacenamiento iniciales, realice esta tarea.

Requisitos previos

- Antes de eliminar una directiva de almacenamiento del VMware vCenter o de un espacio de nombres de vSphere, o de cambiar la asignación de la directiva de almacenamiento, asegúrese de que no haya ninguna notificación de volumen persistente con la clase de almacenamiento correspondiente en el espacio de nombres. Asimismo, asegúrese de que ningún clúster de Tanzu Kubernetes esté utilizando la clase de almacenamiento.
- Si el espacio de nombres se encuentra en un Supervisor de tres zonas, utilice directivas con reconocimiento de topología. No se pueden asignar directivas de almacenamiento sin reconocimiento de topología al espacio de nombres de tres zonas.

Procedimiento

1 En el vSphere Client, navegue al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Haga clic en la pestaña **Almacenamiento** y, a continuación, en **Directivas de almacenamiento**.

3 Haga clic en el icono **Editar** para cambiar las asignaciones de directivas de almacenamiento.

Agregar directivas de seguridad a un espacio de nombres de vSphere de NSX

Un Supervisor que utiliza redes de NSX admite directivas de seguridad de red configuradas a través de una CRD de directiva de seguridad.

Crear una directiva de seguridad

Como integrante de desarrollo y operaciones, puede configurar el CRD de la directiva de seguridad para aplicar una directiva de seguridad basada en NSX a un espacio de nombres de Supervisor. La directiva de seguridad protege el tráfico de los pods de vSphere y las máquinas virtuales. Las máquinas virtuales incluyen nodos de clústeres de TKG y otras máquinas virtuales implementadas en el Supervisor.

Requisitos previos

Utilice la versión 3.2 o posterior de NSX.

Procedimiento

1 Cree un CRD de directiva de seguridad.

   Para ver los campos que se deben usar y los ejemplos de CRD, consulte la documentación del CRD de directiva de seguridad de operador NSX en GitHub.

2 Acceda al espacio de nombres en el entorno de Kubernetes.

   Consulte Obtener y utilizar el contexto del supervisor.

3 Aplique la directiva de seguridad al espacio de nombres.

```
kubectl apply -f policy-name.yaml
```

4 Vea su directiva de seguridad.

a Vea los detalles de la directiva de seguridad.

```
kubectl get securitypolicy policy-name
```

b Vea una descripción de la directiva de seguridad.

```
kubectl describe securitypolicy policy-name
```

Resultados

También puede utilizar la interfaz de usuario de NSX para ver los detalles de la directiva. Para obtener más información, consulte la página *Documentación de VMware NSX*.

Configurar parámetros de red y de equilibrador de carga para un espacio de nombres

vSphere IaaS control plane no admite la edición del archivo de configuración de NCP `ncp.ini`. Puede crear definiciones de recursos personalizados (Custom Resource Definitions, CRD) en NCP para configurar los parámetros de red y de equilibrador de carga.

CRD de NCPSetting

Cree una CRD de **NCPSetting** y establezca los valores para la configuración de NCP.

En la siguiente tabla se describen los parámetros de red y de equilibrador de carga que puede configurar:

Parámetro	Descripción
`log_dropped_traffic`	Indique si se han registrado las reglas DENY del firewall distribuido. Valores: `True`, `False` El valor predeterminado es `false`
`log_firewall_traffic`	Indique si se han registrado las reglas de DFW. Los valores son: ■ `ALL`. Habilita el registro de todas las reglas de DFW. ■ `DENY`. Habilita el registro solo para reglas DENY.

Parámetro	Descripción
`pool_algorithm`	Opción para establecer el algoritmo de equilibrio de carga en el objeto del grupo de equilibradores de carga. Los valores son: ■ Round_Robin ■ Weighted_Round_Robin ■ Least_Connection ■ Weighted_Least_Connection ■ IP-Hash El valor predeterminado es Round-Robin.
`service_size`	Opción para establecer el tamaño del equilibrador de carga. Los valores son `Small`, `Medium` y `Large`. El valor predeterminado es `Small`.
`l7_persistence`	Opción para establecer la opción de persistencia del equilibrador de carga. Los valores son: ■ `cookie`. ■ `source_ip`
`l7_persistence_timeout`	Valor de tiempo de espera de persistencia en segundos en el perfil de persistencia de capa 7.
`cookie_name`	Especifique un nombre de cookie cuando `l7_persistence type` esté establecido en `cookie`.
`x_forward_for`	Habilite X_forward_for para los encabezados de entrada. Los valores son: ■ `Insert` ■ `Replace`
`snat_rule_logging`	Opción para seleccionar el registro de las reglas SNAT. Los valores son: ■ `None` ■ `Basic`. Registro de todos los espacios de nombres. ■ `Extended`. Registro de todos los espacios de nombres y servicios.
`vs_access_log`	Propiedades de registro del servidor virtual de entrada y ruta. Los valores son: ■ `VS_access_log_none` ■ `access_log_enabled`. Habilita el registro del servidor virtual de capa 7. ■ `log_significant_event_only`. Las solicitudes con un estado de respuesta HTTP >=400 se tratan como un evento significativo. El valor predeterminado es `VS_access_log_none`.
`ip_reallocation_time`	Tiempo en segundos antes de que se pueda reasignar una IP liberada.

Para obtener más información sobre NCP y los objetos de NSX, consulte la documentación de *NSX*.

Realice los siguientes pasos para habilitar esta función:

1 Establezca el valor de **enable_ncp_setting_crd** en **True**.

2 Cree un archivo YAML con la siguiente plantilla:

```
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  name: ncpsettings.vmware.com
spec:
  group: vmware.com
  versions:
    - name: v1
      served: true
      storage: true
      schema:
        openAPIV3Schema:
          type: object
            properties:
              spec:
                type: object
                properties:
                  nsx_v3:
                    type: object
                    properties:
                      log_dropped_traffic:
                        description: 'Indicates whether distributed firewall DENY rules
are logged.'
                        type: boolean
                      log_firewall_traffic:
                        description: 'Indicate whether DFW rules are logged.'
........ All configs that are allow to be configured via CRD........

  scope: Cluster
  names:
    plural: ncpsettings
    singular: ncpsetting
    kind: NCPSetting
    shortNames:
    - ncpstg
```

Por ejemplo:

```
apiVersion: vmware.com/v1alpha2
kind: NCPSetting
metadata:
    name: ncp-setting-crd
spec:
    nsx_v3:
        log_dropped_traffic: True
```

```
         log_firewall_traffic: ALL
         pool_algorithm: Round_Robin
         l7_persistence: cookie
         x_forwarded_for: Insert
```

3 Aplique el archivo YAML con el siguiente comando:

```
kubectl apply -f ncp-setting-crd.yaml.j2
```

Para evitar que varias CRD anulen el mismo valor de configuración, NCP solo procesa el objeto de CRD con el nombre **ncp-setting-crd**. Otras CRD con nombres diferentes se anotan con errores y NCP no las procesa.

Anular la configuración de NCP

Los parámetros de configuración de la CRD pueden tener objetos NSX correspondientes. Cuando se crea una CRD para anular los parámetros, la CRD no cambia los parámetros en los objetos, excepto en los siguientes casos:

- `l7_persistence`, `l7_persistence_timeout` y `cookie_name`. Si la CRD cambia el parámetro `l7_persistence`, NCP crea un nuevo perfil de persistencia con los valores de `l7_persistence`, `l7_persistence_timeout` y `cookie_name`.

  Si los parámetros `l7_persistence_timeout` y `cookie_name` se cambian a través de la CRD, el perfil existente se actualiza en función de los nuevos valores.

- `x_forwarded_for`. Si la CRD cambia el parámetro `x_forwarded_for`, NCP crea un nuevo perfil de aplicación basado en su valor.
- `vs_access_log`. Si la CRD cambia el parámetro `vs_access_log`, NCP actualiza la opción de registro de los servidores virtuales según corresponda.

Administrar servicios de supervisor con vSphere IaaS control plane

4

servicios de supervisor son operadores de Kubernetes certificados por vSphere que ofrecen a los desarrolladores componentes de infraestructura como servicio y servicios de proveedores de software independientes perfectamente integrados. Puede instalar y administrar servicios de supervisor en el entorno de vSphere IaaS control plane para que estén disponibles para su uso con cargas de trabajo.

Cuando se instalan servicios de supervisor en Supervisores, los ingenieros de desarrollo y operaciones pueden consumirlos de diferentes maneras:

- Los servicios de supervisor compartidos, como Harbor, proporcionan funcionalidad directamente a las cargas de trabajo que se ejecutan en clústeres de TKG, pods de vSphere o máquinas virtuales.
- Los servicios de supervisor que incluyen un operador, como MinIO, suelen proporcionar interfaces de API o gráficas que los ingenieros de desarrollo y operaciones pueden utilizar para crear y administrar instancias del servicio en un espacio de nombres de vSphere a través de CRD. Por ejemplo, para crear un depósito MiniIO, puede utilizar un CRD para crear el depósito en un espacio de nombres de vSphere.

Obtenga más información sobre las instancias de servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Implementaciones de Supervisor compatibles con servicios de supervisor

Los servicios de servicios de supervisor se implementan como pods de vSphere. En la versión vSphere 8.0, solo los Supervisores configurados con la pila de redes NSX admiten pods de vSphere y sus respectivos servicios de supervisor. A partir de la versión vSphere 8 Update 1, se admiten los pods de vSphere implementados por servicios de supervisor en Supervisores implementados con ambos tipos de redes, NSX o VDS.

Nota Cuando Supervisor se encuentra configurado con la pila de redes de VDS, no se pueden ejecutar instancias de servicios de supervisor en redes respaldadas por NSX (grupos de puertos distribuidos creados por NSX).

En la siguiente tabla, se enumera la compatibilidad con pods de vSphere implementados por servicios de supervisor en las implementaciones de Supervisor existentes para vSphere 8 y versiones posteriores:

Versión de vSphere	Redes NSX	Redes de VDS	Versión de Supervisor	Supervisor de zona única	Supervisor de tres zonas
vSphere 8	yes	no	1.23 y versiones posteriores	yes	no
vSphere 8.0.1 y versiones posteriores	yes	yes	1.24 y versiones posteriores	yes	no
vSphere 8.0.3 y versiones posteriores	yes	yes	1.28 y versiones posteriores	yes	yes

Administración del ciclo de vida de servicios de supervisor

Puede administrar servicios de supervisor desde vSphere Client. Puede instalar servicios de supervisor en Supervisores, actualizar sus versiones o desinstalar servicios de supervisor de Supervisores. Una instancia de servicio de supervisor puede tener varias versiones registradas con vCenter Server, pero solo puede instalar una versión a la vez en un Supervisor.

Tabla 4-1. Estados de servicio de supervisor

Estado	Versión del servicio	Servicio completo
activa	La versión del servicio está lista para instalarse en Supervisores.	Al menos una versión del servicio está en estado activo.
Desactivada	La versión del servicio no se puede instalar en Supervisores. Puede seguir ejecutándose en Supervisores en los que esté instalado, pero no puede instalar una versión desactivada en nuevos Supervisores.	Cuando toda la instancia de servicio de supervisor está desactivada, todas sus versiones también están desactivadas y no se puede instalar ninguna de ellas en Supervisores ni agregar nuevas versiones de servicio hasta que se reactive el servicio.

La administración del ciclo de vida de un servicio de supervisor incluye las siguientes operaciones:

Operación	Descripción
Agregar un nuevo servicio de supervisor a vCenter Server	Cuando se agrega un nuevo servicio a vCenter Server, el servicio y toda la información sobre él se registran en vCenter Server. El servicio aún no está instalado en ningún Supervisor. Después de registrar el servicio en vCenter Server, su estado es Activo, lo que significa que puede instalar ese servicio en Supervisores.
Agregar una nueva versión de servicio de supervisor a vCenter Server	Una vez que haya agregado una instancia de servicio de supervisor a vCenter Server, puede agregar nuevas versiones de ese servicio. Después de registrar la nueva versión del servicio en vCenter Server, pasa al estado Activo y se puede instalar la versión en Supervisores.
Instalar un servicio de supervisor en Supervisores	Cuando se instala una instancia de servicio de supervisor en Supervisor, el archivo YAML de servicio se aplica a Supervisory se crean todos los pods de vSphere y los recursos necesarios para que funcione el servicio. Se crea automáticamente una instancia de espacio de nombres de vSphere para cada servicio de supervisor que instale en Supervisor. Puede administrar los recursos de servicio desde ese espacio de nombres de vSphere. servicios de supervisor también puede tener un complemento de interfaz de usuario para vCenter Server, donde se puede administrar la configuración del servicio.
Actualizar una instancia de servicio de supervisor	Para actualizar un servicio instalado en un Supervisor, primero agregue una nueva versión de servicio a vCenter Server y, a continuación, instale la nueva versión en el Supervisor. Durante la actualización del servicio, el archivo YAML de la nueva versión se aplica al Supervisor. Se eliminarán todos los recursos especificados en la versión anterior del servicio que no sean necesarios para la nueva versión. Por ejemplo, si la versión 1 especifica el pod A y la versión 2 especifica el pod B, después de la actualización a la versión 2, se crea un nuevo pod B y se elimina el pod A. Ninguna carga de trabajo en ejecución actualmente se ve afectada durante el proceso.
Desinstalar una versión de servicio de supervisor	La desinstalación de una versión de servicio de un Supervisor hace que todos los recursos de servicios se eliminen del clúster, incluido el espacio de nombres de servicio. Las instancias de aplicación del servicio en las cargas de trabajo de Kubernetes seguirán ejecutándose.
Eliminar una versión de servicio de supervisor	Para eliminar una versión del servicio, primero debe desactivar esa versión y desinstalarla de los Supervisores donde se ejecuta. A continuación, puede eliminar la versión del servicio de vCenter Server.
Eliminar un servicio de supervisor completo	Para eliminar un servicio completo, debe desactivar todas sus versiones, desinstalar estas versiones de Supervisores y, por último, eliminar todas las versiones del servicio.

servicios de supervisor básico

Los servicios de supervisor principales son servicios cuyos operadores están preinstalados en vSphere IaaS control plane durante la activación de Supervisor. Puede instalar los servicios de supervisor principales en Supervisores y actualizar sus versiones sin necesidad de actualizar Supervisor primero. Sin embargo, no puede eliminar los operadores de los servicios de supervisor principales de vSphere IaaS control plane.

Algunos ejemplos de servicios de supervisor principales son el servicio TKG y el servicio de operador para vSphere de Velero.

Lea los siguientes temas a continuación:

- Agregar una instancia de servicio de supervisor a vCenter Server
- Instalar servicio de supervisor en Supervisor
- Acceder a la interfaz de administración de un servicio de supervisor en el Supervisor
- Agregar una nueva versión a un servicio de supervisor
- Actualizar una instancia de servicio de supervisor a una versión más reciente
- Ver servicios de supervisor instalados en un Supervisor
- Desactivar un servicio de supervisor o una versión
- Activar una versión de servicio de supervisor en vCenter Server
- Desinstalar servicio de supervisor de Supervisor
- Eliminar una versión del servicio de supervisor
- Eliminar un servicio de supervisor

Agregar una instancia de servicio de supervisor a vCenter Server

Consulte cómo agregar servicios de supervisor al sistema vCenter Server donde se ejecuta el entorno de vSphere IaaS control plane. Después de agregar servicios a vCenter Server, instale servicios de supervisor en Supervisores para que los ingenieros de desarrollo y operaciones puedan utilizar los servicios en las cargas de trabajo de Kubernetes.

- Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega el servicio.

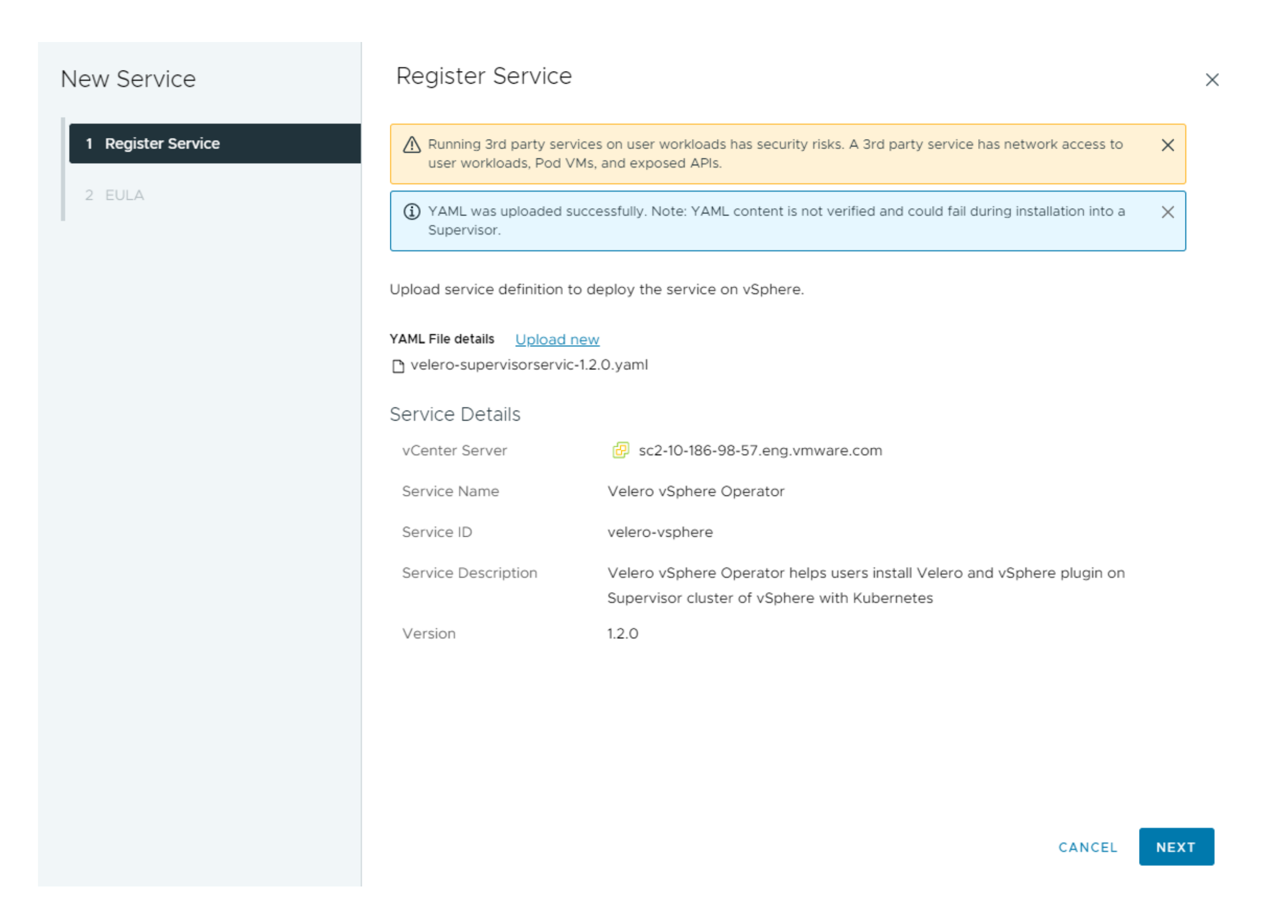
Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 Seleccione un sistema vCenter Server en el menú desplegable de la parte superior.

4 Arrastre y suelte el archivo YAML del servicio en la tarjeta **Agregar nuevo servicio**.

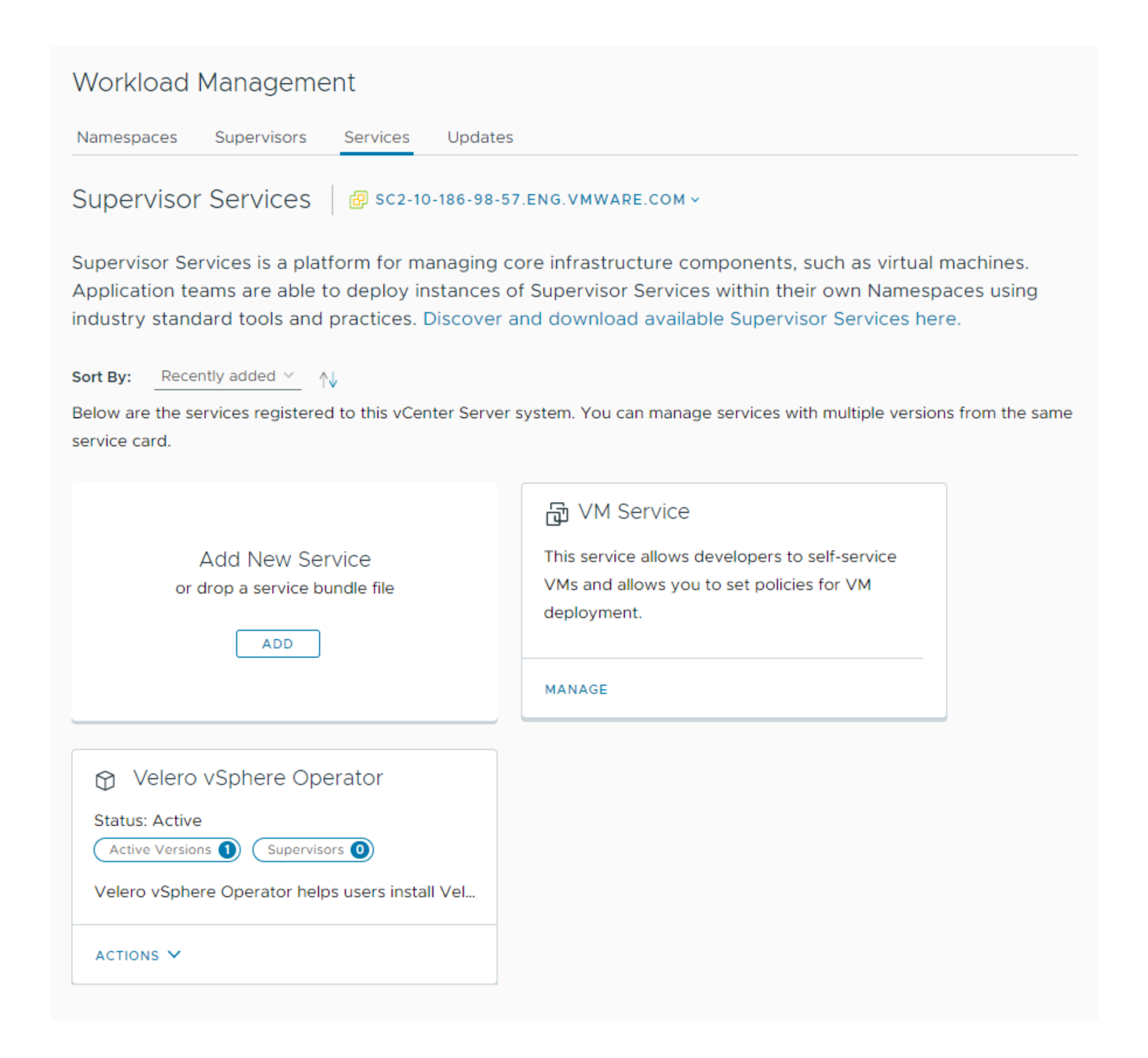


5 Haga clic en **Siguiente** y acepte el CLUF, si existe alguno.

6 Haga clic en **Finalizar**.

Resultados

La instancia de servicio de supervisor y toda su información se registran con el sistema vCenter Server. El servicio está en estado Activo.



Pasos siguientes

Instale la instancia de servicio de supervisor en Supervisores para que los ingenieros de desarrollo y operaciones puedan utilizarlo en las cargas de trabajo de Kubernetes. Consulte Instalar servicio de supervisor en Supervisor.

Instalar servicio de supervisor en Supervisor

Tras agregar un servicio de supervisor en vCenter Server, puede instalarlo en un Supervisor del entorno de vSphere IaaS control plane. Si instala una versión más reciente del servicio de supervisor, este reemplazará cualquier versión de servicio anterior que haya en ese Supervisor. Solo se puede ejecutar una versión de los servicio de supervisor en un Supervisor a la vez.

- Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Requisitos previos

- Agregue un nuevo servicio de supervisor o un servicio existente o de una versión más reciente a vCenter Server. Consulte Agregar una instancia de servicio de supervisor a vCenter Server o Agregar una nueva versión a un servicio de supervisor.
- Compruebe que tiene el privilegio **Administrar servicios de Supervisor en Supervisores** en la instancia de Supervisor donde desea instalar el servicio.
- Si el servicio de supervisor requiere de almacenamiento persistente, configure la plataforma de persistencia de datos de vSAN. Consulte Capítulo 5 Usar la plataforma para la persistencia de datos de vSAN con servicios con estado modernos.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
2 Seleccione **Servicios**
3 En la tarjeta del servicio de supervisor que desea instalar, seleccione **Acciones > Administrar servicio** .
4 En el menú desplegable **Instalar versión**, seleccione la versión de servicio de supervisor.

Nota No puede instalar versiones de servicio de supervisor que estén desactivadas.

5 Seleccione el Supervisor donde desea instalar el servicio.
6 Haga clic en **Siguiente**.

Se realizan comprobaciones previas de compatibilidad para determinar si la versión de servicio de supervisor que desea instalar es compatible con el Supervisor. Si la versión del servicio es compatible con Supervisor, puede continuar con la instalación. En caso de que la versión del servicio seleccionada no sea compatible con el Supervisor, se muestran dos tipos de mensajes que describen la incompatibilidad exacta:

- Mensajes de advertencia. Puede omitir los mensajes de advertencia, pero debe confirmarlos para continuar con la instalación.
- Mensajes de error. Un mensaje de error indica que la versión de servicio de supervisor no es compatible con el Supervisor y no se puede instalar. En caso de que aparezcan mensajes de error, primero debe resolver la incompatibilidad detectada antes de poder instalar el servicio en el Supervisor concreto.

7 En el campo **Configuración de servicio YAML**, introduzca las propiedades de configuración si el servicio requiere alguna.
8 Consulte el progreso de la instalación del servicio en Supervisores.

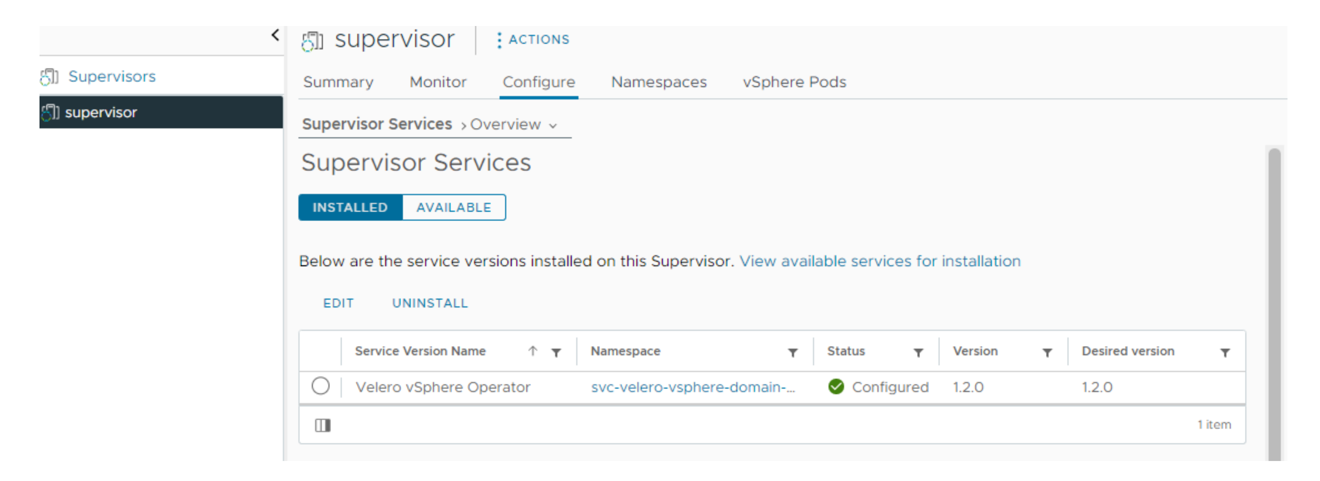
a Seleccione la pestaña **Supervisores** y luego elija una instancia de Supervisor donde instalar el servicio.

b Haga clic en **Configurar** y en **Servicios de supervisor > Descripción general**.

c Seleccione la pestaña **Instalado**.

Resultados

El estado del servicio de supervisor es Configurando, lo que significa que todos los recursos necesarios se crean en el Supervisor y el YAML de servicio se aplica al clúster. Una vez que el YAML se aplique correctamente en el Supervisor con todos sus recursos y el espacio de nombres creados o actualizados, el estado del servicio pasará a ser Configurado. El servicio está disponible para todos los espacios de nombres de ese clúster, y los ingenieros de desarrollo y operaciones pueden utilizarlo con sus cargas de trabajo.



Pasos siguientes

Configure el servicio de supervisor mediante la interfaz. Consulte dónde se puede encontrar en Acceder a la interfaz de administración de un servicio de supervisor en el Supervisor.

Acceder a la interfaz de administración de un servicio de supervisor en el Supervisor

Compruebe dónde encontrar la interfaz de usuario de administración de servicios de supervisor una vez que la instale en un Supervisor. Los servicios de supervisor pueden proporcionar su propio complemento de interfaz de usuario para vCenter Server que agrega la interfaz de servicio a la vista del Supervisor en vSphere Client. En función de los detalles de servicio de supervisor, puede utilizar su interfaz para configurar y administrar el servicio también para implementar instancias de servicio de ese servicio.

Procedimiento

1 En el inventario de vSphere Client, desplácese hasta el clúster de hosts que convirtió en un Supervisor.

2 Haga clic en **Configurar** y desplácese hacia abajo hasta la interfaz de servicio, a la que se le suele poner el nombre del servicio; por ejemplo, **MinIO**.

Agregar una nueva versión a un servicio de supervisor

Una vez que haya agregado un servicio de supervisor a vCenter Server en el que tiene el entorno de vSphere IaaS control plane, puede agregar una nueva versión a ese servicio. Puede instalar diferentes versiones de servicio en Supervisores.

- Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Requisitos previos

- Agregue el servicio a vCenter Server. Consulte Agregar una instancia de servicio de supervisor a vCenter Server.
- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega la nueva versión del servicio.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 En la tarjeta del servicio al que desea agregar una nueva versión, seleccione **Acciones > Agregar nueva versión**.

4 Cargue el archivo YAML de la nueva versión del servicio y haga clic en **Siguiente**.

5 Acepte el CLUF si lo hubiera y haga clic en **Finalizar**.

Resultados

Se agrega la nueva versión del servicio y se encuentra en estado activo.

Pasos siguientes

Instale la nueva versión del servicio en Supervisores. Consulte Instalar servicio de supervisor en Supervisor.

Actualizar una instancia de servicio de supervisor a una versión más reciente

Una vez que haya agregado una nueva versión de servicio de supervisor a vCenter Server, puede instalar esa versión en Supervisores. Solo puede instalar versiones activas de servicio de supervisor y compatibles con los Supervisores en los que desea instalarlas. Se realizan comprobaciones previas de compatibilidad para garantizar que la nueva versión de servicio de supervisor sea compatible con el Supervisores de destino.

Requisitos previos

- Agregar la nueva versión de servicio de supervisor a vCenter Server. Consulte Agregar una nueva versión a un servicio de supervisor.

- Compruebe que tiene el privilegio **Administrar servicios de Supervisor en Supervisores** en la instancia de Supervisor donde desea instalar el servicio.

Procedimiento

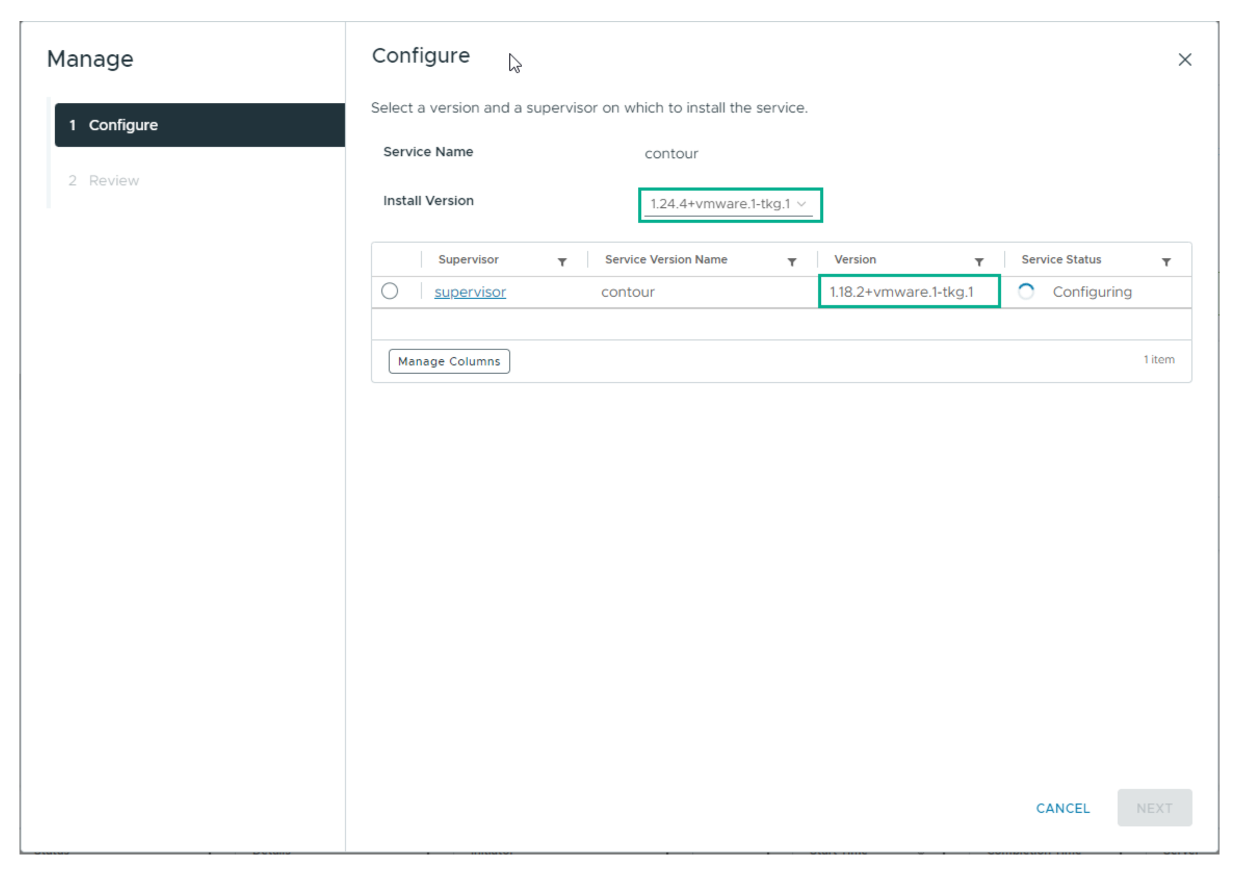
1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 Seleccione **Gestionar servicio**.

4 Seleccione la nueva versión que desea instalar y seleccione la instancia de Supervisor donde desea instalarla.

   Compruebe que la versión del servicio instalada actualmente en Supervisor sea anterior.



5 Haga clic en **Siguiente**.

   Se realizan comprobaciones previas de compatibilidad para determinar si la versión de servicio de supervisor que desea instalar es compatible con el Supervisor. Si la versión del servicio es compatible con Supervisor, puede continuar con la instalación. En caso de que la versión del servicio seleccionada no sea compatible con el Supervisor, se muestran dos tipos de mensajes que describen la incompatibilidad exacta:

   - Mensajes de advertencia. Puede omitir los mensajes de advertencia, pero debe confirmarlos para continuar con la instalación.

- Mensajes de error. Un mensaje de error indica que la versión de servicio de supervisor no es compatible con el Supervisor y no se puede instalar. En caso de que aparezcan mensajes de error, primero debe resolver la incompatibilidad detectada antes de poder instalar el servicio en el Supervisor concreto.

6 En el campo **Configuración de servicio YAML**, introduzca las propiedades de configuración si el servicio requiere alguna.

7 Consulte el progreso de la instalación del servicio en Supervisores.

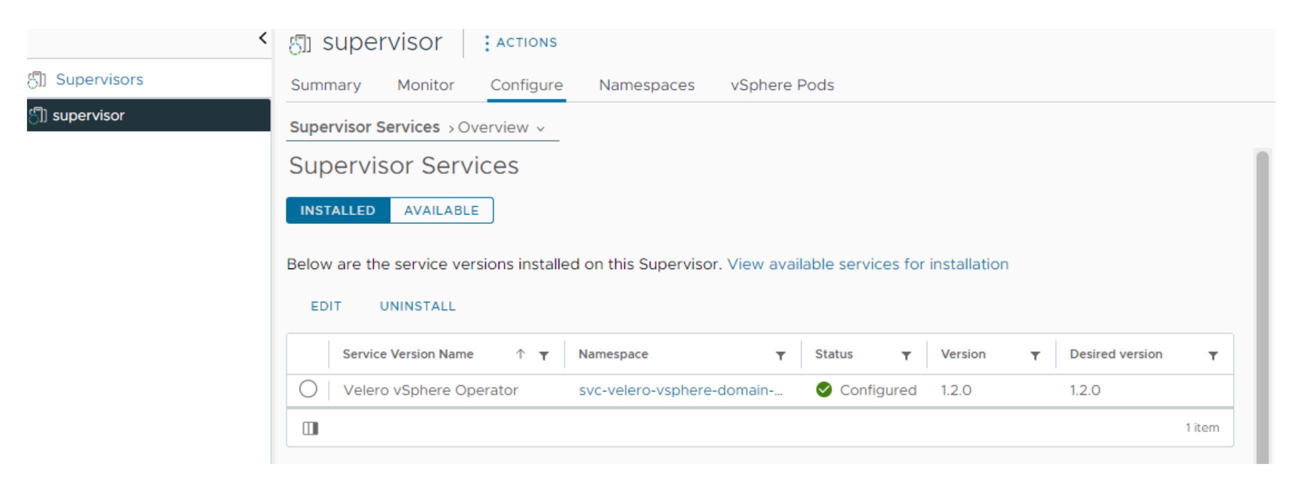
   a Seleccione la pestaña **Supervisores** y luego elija una instancia de Supervisor donde instalar el servicio.

   b Haga clic en **Configurar** y en **Servicios de supervisor > Descripción general**.

   c Seleccione la pestaña **Instalado**.

Resultados

El estado del servicio de supervisor es Configurando, lo que significa que todos los recursos necesarios se crean en el Supervisor y el YAML de servicio se aplica al clúster. Una vez que el YAML se aplique correctamente en el Supervisor con todos sus recursos y el espacio de nombres creados o actualizados, el estado del servicio pasará a ser Configurado. El servicio está disponible para todos los espacios de nombres de ese clúster, y los ingenieros de desarrollo y operaciones pueden utilizarlo con sus cargas de trabajo.



Ver servicios de supervisor instalados en un Supervisor

Vea los servicios de vSphere instalados en los Supervisores del entorno de vSphere IaaS control plane. Los servicios de supervisor instalados en un Supervisor están disponibles para cada espacio de nombres en el clúster.

Requisitos previos

- Agregue servicios de supervisor a vCenter Server. Consulte Agregar una instancia de servicio de supervisor a vCenter Server.

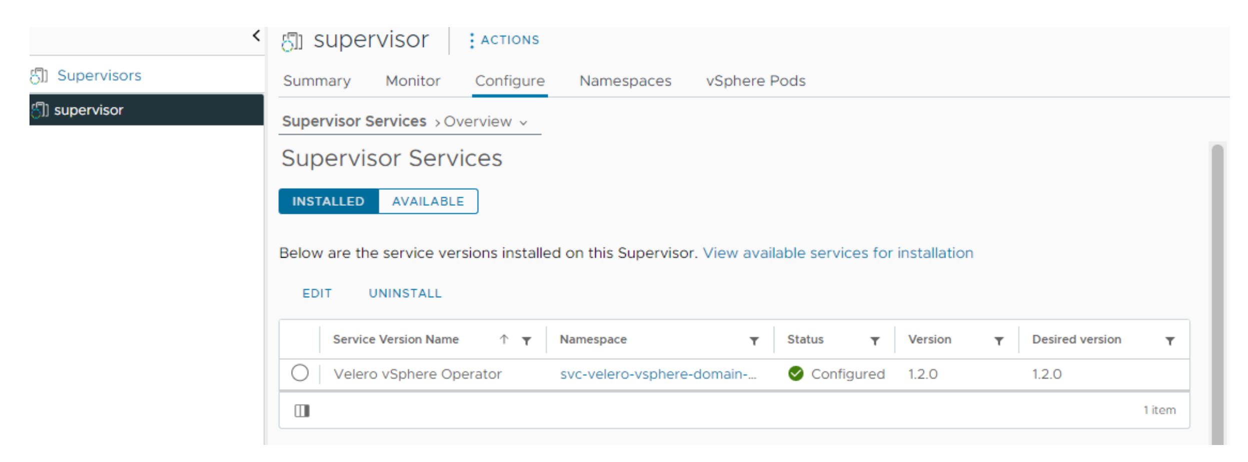
- Instale servicios de supervisor en Supervisores. Consulte Instalar servicio de supervisor en Supervisor.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Haga clic en la pestaña **Supervisores** y seleccione un Supervisor de la lista.

3 Haga clic en la pestaña **Configurar** y en **Descripción general**, en **Servicios de supervisor**.



- En la pestaña **Instalado**, vea los servicios de supervisor que están instalados actualmente en el Supervisor.
- En la pestaña **Disponible**, vea los servicios de supervisor disponibles para instalación.

Pasos siguientes

Puede administrar los servicios de supervisor en ese Supervisor, desinstalar servicios o instalar otros nuevos desde los servicios en la pestaña **Disponible**.

Desactivar un servicio de supervisor o una versión

Desactive una versión del servicio de supervisor si ya no desea utilizarla con cargas de trabajo de Kubernetes en su entorno de vSphere IaaS control plane. Una versión de servicio desactivada sigue ejecutándose en los Supervisores en los que se ha instalado, pero no es posible instalar una versión de servicio desactivada en otros Supervisores. Cuando se desactiva un servicio completo, todas las versiones del servicio se desactivan, por lo que no es posible agregar nuevas versiones de servicio ni instalarlas en los Supervisores hasta que se reactive el servicio.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el nivel de vCenter Server.

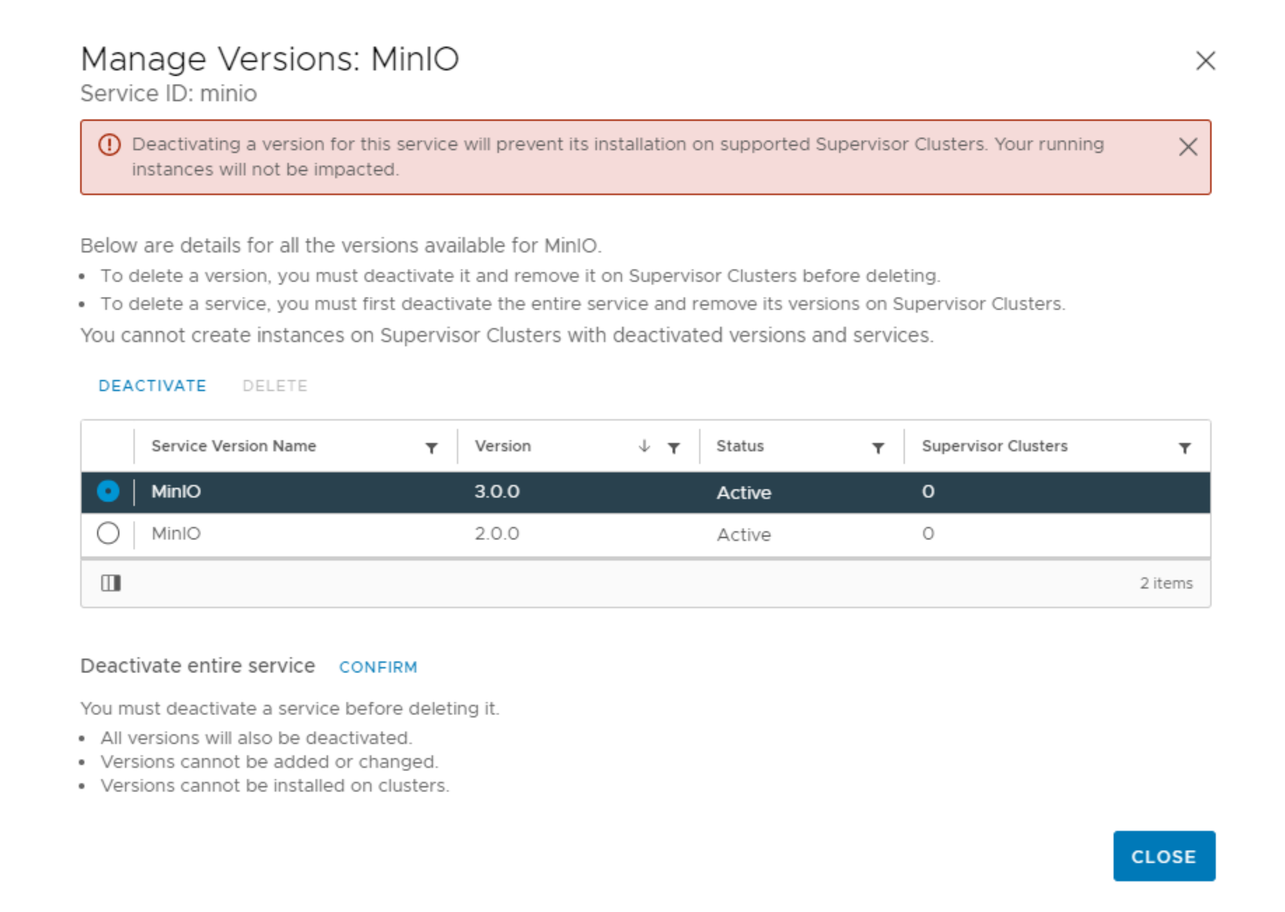
Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 En la tarjeta de servicio, seleccione **Acciones > Administrar versiones**.

- Para desactivar una versión del servicio de supervisor, seleccione la versión y haga clic en **Desactivar**.
- Para desactivar todo el servicio, haga clic en **Confirmar** junto a **Desactivar todo el servicio**.



Resultados

La versión del servicio está desactivada y no es posible instalar en los Supervisores.

Activar una versión de servicio de supervisor en vCenter Server

Una vez que se desactiva una versión de servicio de supervisor, puede volver a activarla en caso de que el equipo de desarrollo y operaciones desee utilizar esa versión de servicio en las cargas de trabajo de Kubernetes que se ejecutan en vSphere IaaS control plane.

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server en el que está registrado el servicio.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 En la tarjeta de servicio de supervisor, haga clic en **Versiones activas**.

4 Seleccione **Administrar versiones**.

5 Seleccione la versión de servicio de supervisor en estado Desactivado y haga clic en **Reactivar**.

Desinstalar servicio de supervisor de Supervisor

Desinstale servicio de supervisor de Supervisor si el equipo de desarrollo y operaciones ya no necesita ese servicio para las cargas de trabajo de Kubernetes que se ejecutan en el entorno de vSphere IaaS control plane.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server que aloja la instancia de Supervisor en la que está instalado el servicio.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Haga clic en la pestaña **Supervisores** y seleccione un Supervisor de la lista.

3 Haga clic en la pestaña **Configurar** y en **Descripción general**, en **Servicios de supervisor**.

4 En **Instalado**, seleccione la instancia de servicio de supervisor que desea desinstalar y haga clic en **Desinstalar**.

Resultados

servicio de supervisor se desinstala de Supervisor. Todos los recursos de servicios y el espacio de nombres de servicio se eliminan del Supervisor. Todas las instancias administradas de servicios que utilizan la plataforma de persistencia de datos vSAN se eliminan del Supervisor.

Eliminar una versión del servicio de supervisor

Elimine la versión de un servicio de supervisor de vCenter Server si esta versión está obsoleta y su equipo de desarrollo y operaciones ya no la necesita para la carga de trabajo de Kubernetes que se ejecuta en el entorno de vSphere IaaS control plane.

Requisitos previos

- Compruebe que la versión del servicio de supervisor que desea eliminar no está instalada en Supervisores. Consulte Desinstalar servicio de supervisor de Supervisor.

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el nivel de vCenter Server.

Procedimiento

1. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
2. Seleccione **Servicios**
3. En la tarjeta del servicio de supervisor, seleccione **Acciones > Administrar versiones**.
4. Seleccione la versión que desee eliminar y haga clic en **Desactivar**.
5. Seleccione la versión desactivada y haga clic en **Eliminar**.

Eliminar un servicio de supervisor

Elimine un servicio de supervisor del entorno de vSphere IaaS control plane si sus ingenieros de desarrollo y operaciones ya no lo necesitan para sus cargas de trabajo de Kubernetes.

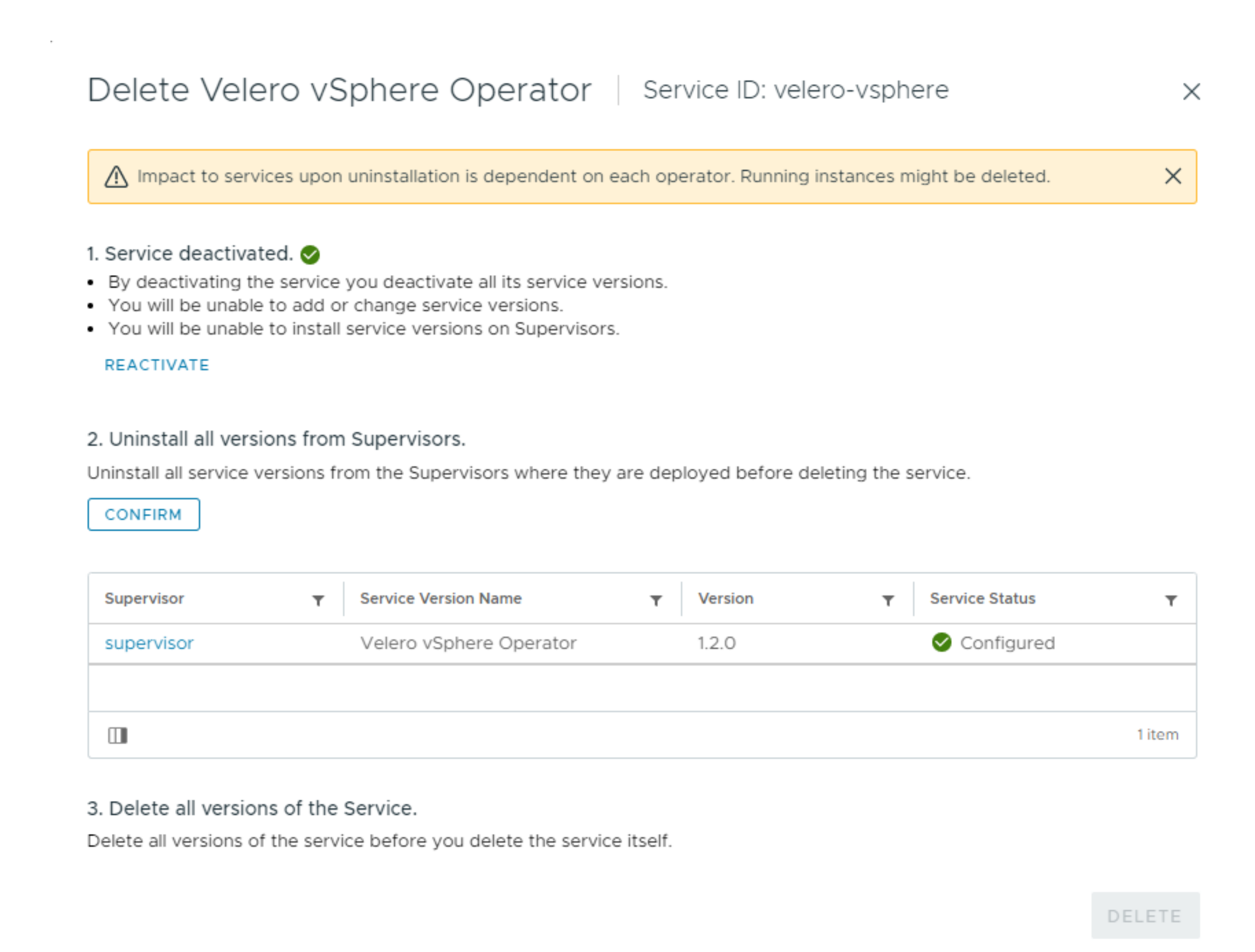
Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server en el que está registrado el servicio.

Procedimiento

1. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
2. Seleccione **Servicios**
3. En la tarjeta del servicio de supervisor que desea eliminar, seleccione **Acciones > Eliminar**.
4. Confirme la desactivación de todas las versiones de servicio disponibles actualmente.
5. Confirme la desinstalación del servicio de los Supervisores.

   La desinstalación de un servicio de supervisor del Supervisores en el que se ejecuta puede tardar algún tiempo. Puede cerrar el cuadro de diálogo mientras se completa el proceso y, a continuación, volver a abrirlo para continuar con la siguiente fase.



6 Confirme la eliminación de todas las versiones disponibles del servicio.

7 Haga clic en **Eliminar**.

Usar la plataforma para la persistencia de datos de vSAN con servicios con estado modernos

5

En vSphere IaaS control plane, es posible utilizar la plataforma de persistencia de datos de vSAN para servicios con estado modernos que requieren almacenamiento persistente. La plataforma proporciona un marco que permite que los terceros integren sus aplicaciones de servicio con la infraestructura de vSphere subyacente.

Acerca de persistencia de datos de vSAN Plataforma

Entre las ventajas de usar la persistencia de datos de vSAN se incluyen las siguientes:

Implementación y ampliación automáticas de servicios

Con vSphere Client, los administradores pueden instalar e implementar un servicio con estado moderno en un Supervisor y conceder acceso al espacio de nombres del servicio a los ingenieros de desarrollo y operaciones. Los ingenieros de desarrollo y operaciones pueden aprovisionar y ampliar instancias del servicio con estado de forma dinámica como si fuera un autoservicio a través de las API de Kubernetes.

Supervisión de servicios integrada con vCenter Server

Los partners pueden crear complementos de paneles de control que se integren con vCenter Server. Con estos complementos de interfaz de usuario, los administradores de vSphere pueden administrar y supervisar los servicios con estado. Además, vSAN ofrece funciones de supervisión de estado y capacidad para estos servicios de terceros integrados.

Configuración de almacenamiento optimizada con vSAN Direct

vSAN Direct habilita los servicios con estado moderno para que se conecten directamente con el almacenamiento de conexión directa subyacente y, de este modo, optimizar la eficiencia de E/S y el almacenamiento.

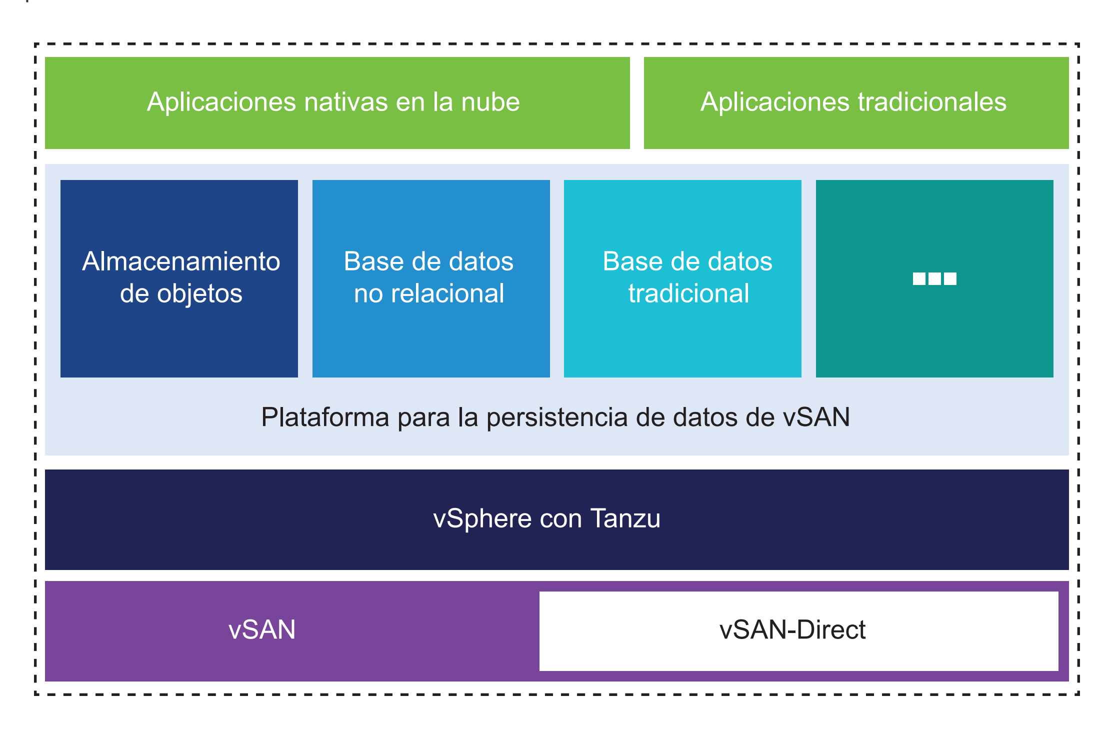
La plataforma admite los siguientes tipos de servicios:

- Almacenamiento de objetos, como MinIO.
- Las bases de datos de NoSQL, también denominadas bases de datos no relacionales.
- Bases de datos tradicionales.

Almacenamiento que no comparte nada de vSphere

La mayoría de servicios con estado modernos tienen una arquitectura de no compartir nada (Shared Nothing Architecture, SNA). Consumen almacenamiento local no replicado y ofrecen sus propios servicios de replicación de almacenamiento, compresión y otras operaciones de datos. Como resultado, los servicios no aprovechan que las mismas operaciones se hayan ya realizado en el almacenamiento subyacente.

Para evitar duplicar las operaciones, la plataforma para la persistencia de datos de vSAN ofrece dos soluciones vSAN con rutas de datos optimizadas. El servicio persistente puede entonces ejecutarse en vSAN con la directiva de almacenamiento de SNA o en un almacenamiento local prácticamente sin formato denominado vSAN Direct.



vSAN con la directiva de almacenamiento de SNA

Con esta tecnología, puede usar un almacén de datos de vSAN replicado distribuido con la directiva de SNA de host local vSAN. Como resultado, la aplicación del servicio de SNA puede controlar la colocación y asumir la responsabilidad de mantener disponibles los datos. Con la tecnología, al servicio persistente le resulta más fácil coubicar su instancia de recurso informático y un objeto de almacenamiento en el mismo host ESXi físico. Con la colocación de host-local, es posible realizar operaciones como la replicación en la capa de servicio y no en la capa de almacenamiento.

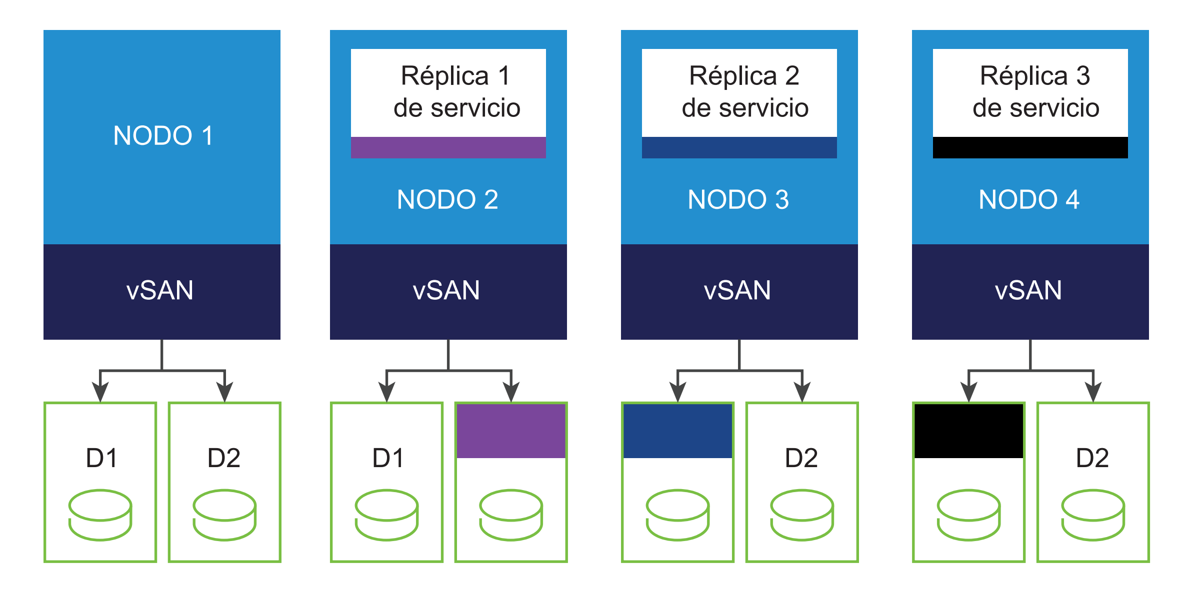
La instancia de recurso informático, como un pod, aparece primero en uno de los nodos del clúster de vSAN. A continuación, el objeto de vSAN creado con la directiva de SNA de vSAN tendrá automáticamente todos los datos colocados en el mismo nodo en el que se ejecuta el pod.

En el siguiente ejemplo se muestra la implementación de almacenamiento de una aplicación que utiliza la clase de almacenamiento de SNA para su volumen persistente. vSAN puede seleccionar cualquier grupo de discos en el nodo para la colocación de volúmenes persistentes.

Total de copias de datos = 3

Tolerancia a errores esperada = 2

Errores reales que se toleran de forma garantizada = 2

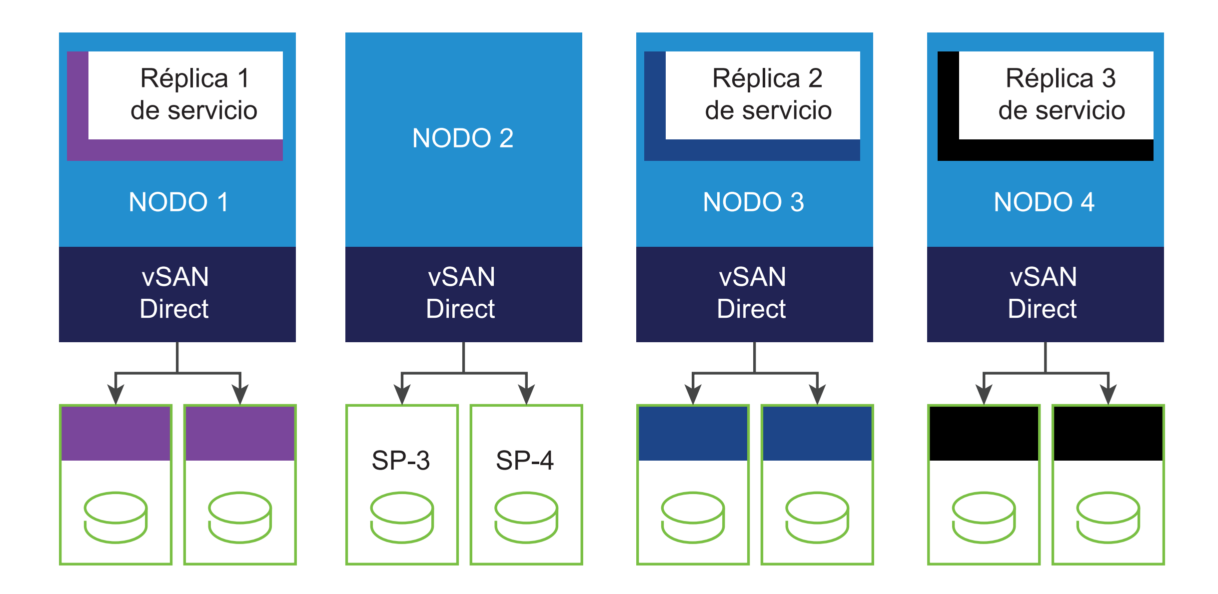


vSAN Direct

A pesar de que vSAN con la directiva de almacenamiento de SNA pueden colocar datos de forma local en la instancia de recurso informático, existe una sobrecarga de una ruta de datos de vSAN distribuida entre la aplicación y el dispositivo de almacenamiento físico. Con vSAN Direct, las aplicaciones de servicios con estado pueden acceder en su mayoría al almacenamiento local sin formato de vSAN a través de una ruta de acceso de datos más directa, la cual ofrece la solución optimizada de mayor rendimiento.

Con vSAN Direct, el administrador de vSphere puede reclamar dispositivos de host-local y, a continuación, administrar y supervisar los dispositivos. vSAN Direct proporciona información sobre el estado, el rendimiento y la capacidad de los dispositivos. En cada dispositivo local que reclama, vSAN Direct crea un almacén de datos de VMFS independiente y lo pone a disposición de la aplicación como una opción de colocación. Los almacenes de datos de VMFS que administra vSAN Direct se muestran como grupos de almacenamiento en Kubernetes. En vSphere Client, aparecen como almacenes de datos de vSAN Direct.

A continuación se muestran los volúmenes persistentes colocados en local en los discos de vSAN Direct.



Cuándo hay que utilizar vSAN con SNA o vSAN Direct

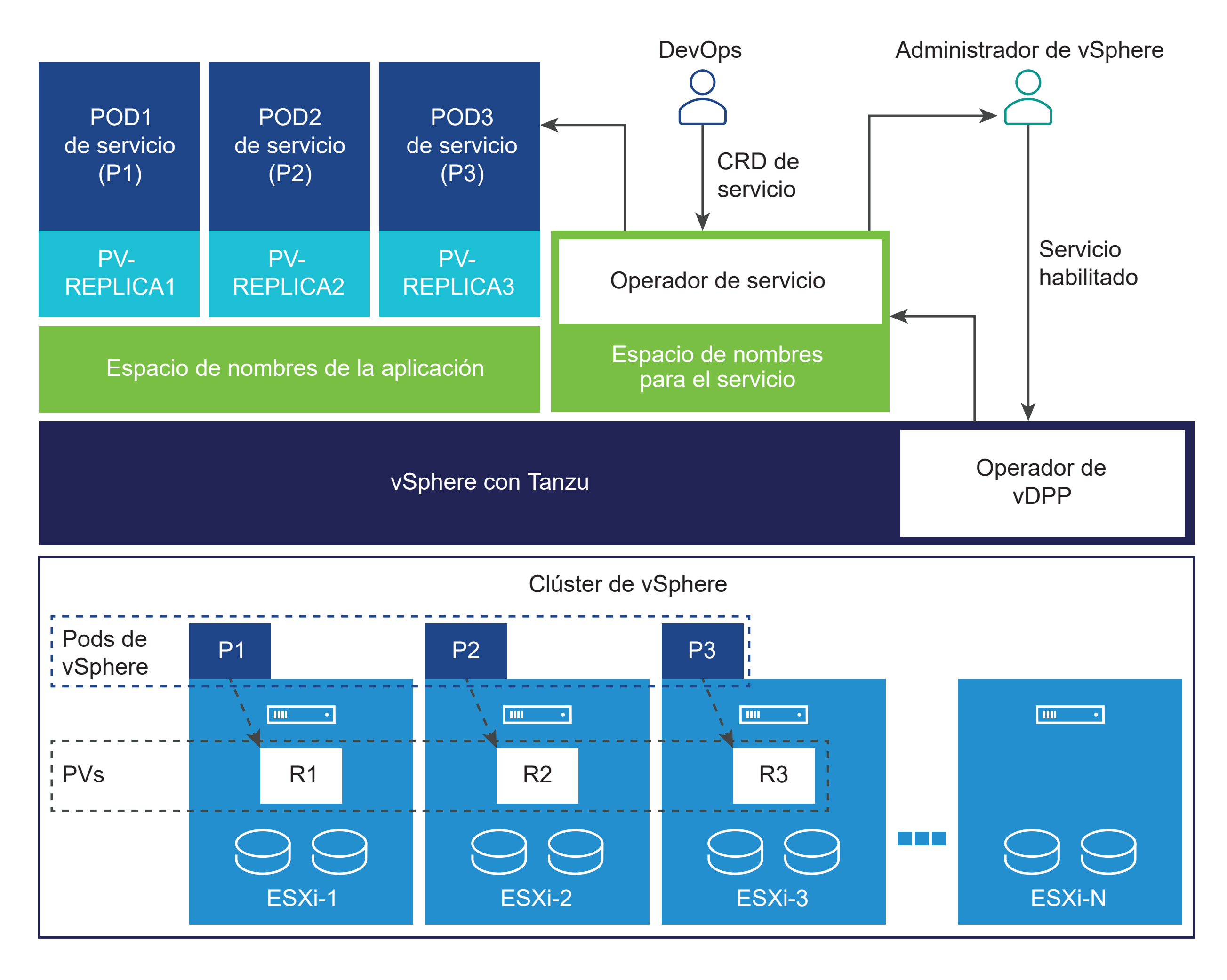
Siga estas recomendaciones generales a la hora de decidir qué tipo de vSAN debe utilizar.

- Utilice vSAN con SNA cuando quiera que la aplicación con estado nativa en la nube comparta la infraestructura física con otras máquinas virtuales comunes o con cargas de trabajo de Kubernetes. Cada carga de trabajo puede definir su propia directiva de almacenamiento y puede obtener lo mejor de ambos mundos desde un solo clúster.
- Use vSAN Direct, en cambio, si va a crear un clúster de hardware dedicado para los servicios nativos en la nube que no comparten nada.

Operador de la plataforma para la persistencia de datos de vSAN

El operador de la plataforma para la persistencia de datos de vSAN (vDPP, vSAN Data Persistence Platform) es un componente que se encarga de ejecutar y administrar los servicios con estado de partners integrados con vSphere. El operador de vDPP muestra los servicios con estado disponible al administrador de vSphere. Cuando el administrador de vSphere habilita un servicio persistente (por ejemplo, MinIO), el operador de vDPP implementa un operador específico de la aplicación para el servicio en el Supervisor.

Los operadores específicos de la aplicación son proporcionados por el tercero y deben ser compatibles con la vDPP. Por lo general, el operador ofrece un CRD que proporciona una interfaz de autoservicio con la que los usuarios de Kubernetes pueden crear instancias. vSphere IaaS control plane usa este operador y el CRD para aprovisionar nuevas instancias de servicio, además de poder administrarlas y supervisarlas a través de la capa de servicios con estado. La mayoría de estos operadores utilizan conjuntos con estado para implementar sus instancias.



Una vez que el administrador de vSphere habilita un servicio, tiene lugar lo siguiente.

- El operador de vDPP activa un operador específico del servicio.
- El operador específico del servicio registra el complemento de la interfaz de usuario.
- Se crean directivas de almacenamiento optimizadas para el almacenamiento.

Límites de configuración para la plataforma de persistencia de datos de vSAN

VMware proporciona límites de configuración en la herramienta Valores máximos de configuración de VMware.

Valores máximos de persistencia de datos de vSAN	Límites
Cantidad máxima de volúmenes persistentes por plataforma de persistencia de datos de vSAN	1.000
Cantidad máxima de volúmenes persistentes por instancia de servicio en la plataforma de persistencia de datos de vSAN	De 60 a 80

Lea los siguientes temas a continuación:

- Habilitar servicios con estado en vSphere IaaS control plane
- Configurar un almacén de datos vSAN Direct para servicios con estado
- Supervisar servicios con estado en vSphere IaaS control plane
- Comprobar las directivas de almacenamiento disponibles para los servicios con estado
- Crear directivas de almacenamiento personalizadas para la plataforma de persistencia de datos de vSAN

Habilitar servicios con estado en vSphere IaaS control plane

vSphere IaaS control plane se integra con varios servicios de terceros que utilizan la plataforma de persistencia de datos de vSAN para satisfacer sus necesidades de almacenamiento persistente. Como administrador de vSphere, habilite los servicios en vCenter Server. Cuando habilite el servicio con estado, primero debe registrar el servicio con vCenter Server mediante el archivo YAML descargado que describe el servicio. Después, instale el servicio en los Supervisores para que los ingenieros de desarrollo y operaciones puedan utilizar el servicio en las cargas de trabajo de Kubernetes.

Requisitos previos

Privilegio necesario: **Servicios de supervisor.Administrar servicios de supervisor**

Configurar almacenamiento persistente

Con la plataforma de persistencia de datos de vSAN, los servicios con estado pueden utilizar almacenamiento vSAN en los dos modos siguientes:

- vSAN Direct. Para configurar vSAN Direct, consulte Crear un almacén de datos de vSAN Direct.

  Nota En los discos del almacén de datos de vSAN Direct, no se admiten los cambios en el tipo de asignación de volúmenes. Una vez que seleccione el tipo de asignación de volúmenes para los discos del almacén de datos de vSAN Direct, no podrá cambiarlo. Sin embargo, sí es posible cambiar el tipo de asignación de volúmenes para el disco nuevo en operaciones como clonar y reubicar.

- vSAN regular con la directiva de almacenamiento de SNA. Para obtener información sobre cómo configurar el almacenamiento de vSAN, consulte la *Administrar VMware vSAN*.

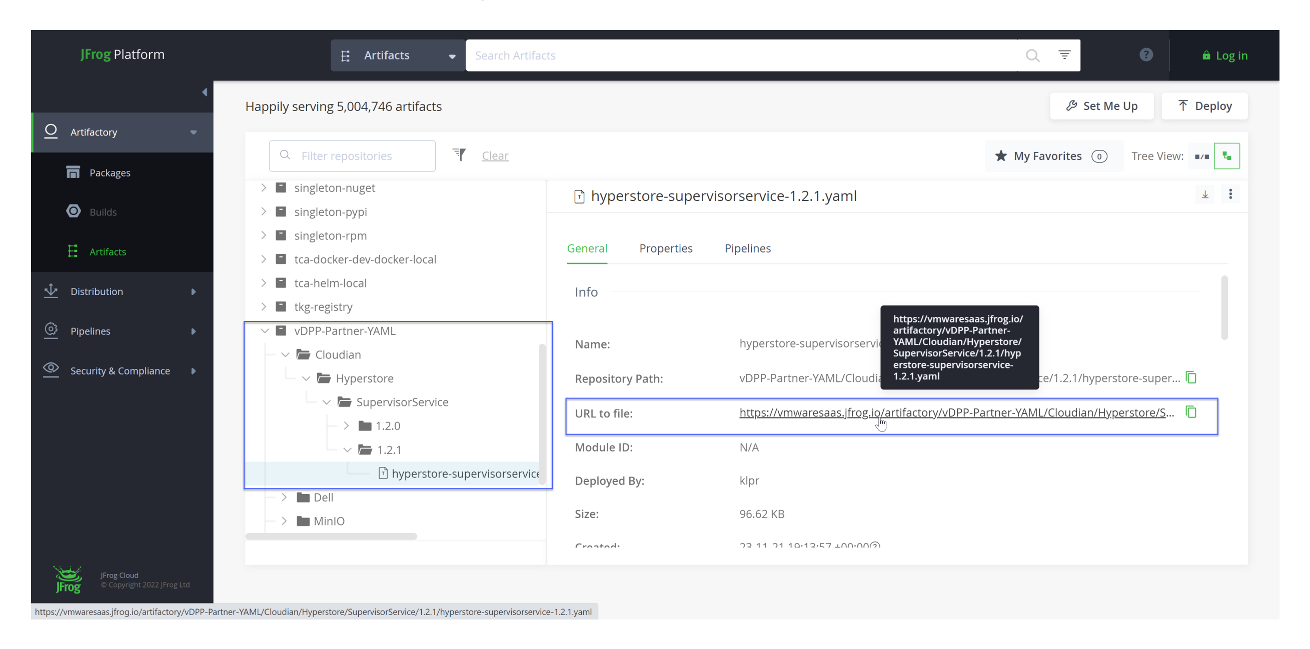
Descargar el archivo YAML del servicio

Cuando descargue los archivos YAML del servicio desde el repositorio que mantiene VMware, asegúrese de utilizar la versión del servicio correcta que es compatible con su versión de vSphere.

Si instaló versiones anteriores de los servicios de partners, MinIO y Cloudian Hyperstore, actualícelas a las versiones compatibles después de actualizar su entorno de vSphere. Las versiones más recientes de los operadores de partners solucionan ciertos problemas y utilizan nuevas funciones de la plataforma. Para obtener más información, consulte la documentación del partner.

1 En el repositorio de https://vmwaresaas.jfrog.io/, vaya a una carpeta de partner adecuada en **Artefactos > vDPP-Partner-YAML**.

2 Haga clic en la URL del archivo y descargue el archivo YAML.



3 Agregar el servicio a vCenter Server

Utilice el archivo YAML del servicio de partners que descargó.

Consulte Agregar una instancia de servicio de supervisor a vCenter Server.

4 Instalar el servicio en el Supervisor

Consulte Instalar servicio de supervisor en Supervisor.

Después de habilitar el servicio, la plataforma persistencia de datos de vSAN realiza las siguientes acciones para crear los recursos necesarios para el servicio:

- Crea un espacio de nombres para este servicio en el Supervisor.
- Crea directivas de almacenamiento predeterminadas y las clases de almacenamiento correspondientes, y las asigna al espacio de nombres.

Las directivas son para almacenes de datos de vSAN Shared-Nothing-Architecture (SNA) y vSAN Direct.

Nota La plataforma de persistencia de datos de vSAN crea automáticamente las clases de almacenamiento vsan-direct y vsan-sna en el espacio de nombres después de que un administrador de vSphere habilite el servicio. Solo las aplicaciones que se ejecutan en el Supervisor pueden utilizar las clases de almacenamiento vsan-direct y vsan-sna. Estas clases de almacenamiento no se pueden utilizar dentro de un clúster de Tanzu Kubernetes Grid.

En vSphere 7.0 Update 2 y otras versiones posteriores, la directiva de almacenamiento vSAN Direct se basa en las capacidades. Si creó directivas basadas en etiquetas en vSphere 7.0 Update 1, estas se convierten automáticamente en directivas basadas en capacidades después de actualizar a vSphere 7.0 Update 2 y otras versiones posteriores.

Si desea crear directivas de almacenamiento personalizadas y asignarlas al espacio de nombres del servicio en lugar de usar las predeterminadas, consulte Crear directiva de almacenamiento de vSAN Direct y Crear directiva de almacenamiento SNA vSAN.

- Crea funciones de desarrollo y operaciones, incluidas las funciones con permisos de edición y visualización.

  Cuando se implementa el operador de servicio, sus objetos CRD personalizados se instalan en el Supervisor. Los usuarios con permiso de edición pueden tener recursos CRUD de estas definiciones de recursos personalizados (Custom Resource Definitions, CRD) en el espacio de nombres. Los usuarios con permiso de vista solo pueden ver los recursos de esta CRD.

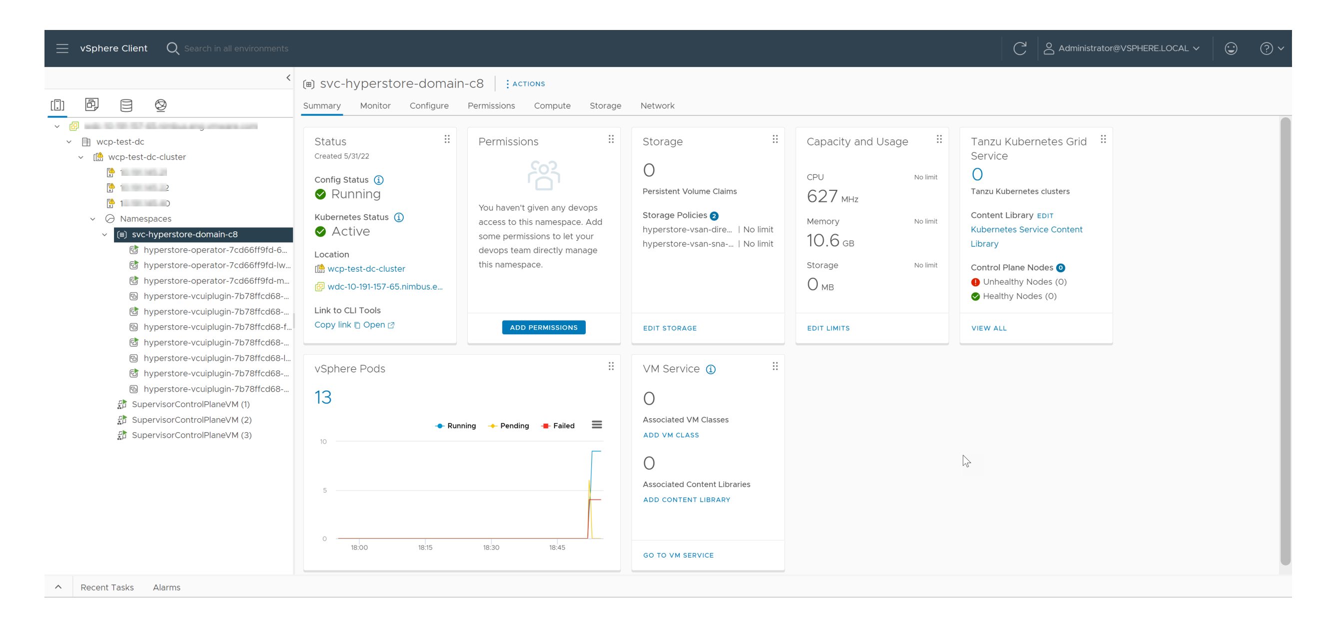
- Si el tercero proporcionó un complemento de interfaz de usuario personalizado, este aparecerá en vSphere Client. El administrador de vSphere puede utilizar el complemento para administrar el servicio.

5 Verificar los recursos creados para el servicio

El administrador de vSphere puede comprobar que se hayan creado todos los recursos adecuados para el servicio.

Desplácese hasta el espacio de nombres creado para el servicio y haga clic en la pestaña **Resumen**.

La página Resumen muestra las directivas de almacenamiento asignadas al espacio de nombres, los pods de vSphere que se ejecutan en el espacio de nombres, etc.



6 Administrar y supervisar el servicio

- Si el tercero proporcionó un complemento de interfaz de usuario personalizado, el administrador de vSphere puede utilizar el complemento para administrar y supervisar el servicio.

  Para obtener más información, consulte la documentación del complemento de interfaz de usuario de tercero.

- Además, el administrador de vSphere puede utilizar las comprobaciones de Skyline Health para supervisar los servicios. Consulte Supervisar servicios con estado en vSphere IaaS control plane.

- Si desea crear directivas de almacenamiento personalizadas en lugar de las predeterminadas, consulte Crear directivas de almacenamiento personalizadas para la plataforma de persistencia de datos de vSAN.

7 Empezar a utilizar el servicio

El ingeniero de desarrollo y operaciones utiliza el comando `kubectl` para acceder al espacio de nombres del servicio.

Para comprobar que el espacio de nombres que utiliza para los servicios con estado tiene las clases de almacenamiento adecuadas, consulte Comprobar las directivas de almacenamiento disponibles para los servicios con estado.

Puede utilizar los CRD de terceros para implementar instancias del servicio de aplicaciones de terceros. Si desea obtener más información, consulte la documentación de terceros.

Configurar un almacén de datos vSAN Direct para servicios con estado

Si desea crear un clúster de hardware dedicado para servicios con estado en vSphere IaaS control plane, puede utilizar un almacén de datos de vSAN Direct. vSAN Direct es un almacén de datos principalmente sin procesar que se implementa en dispositivos de almacenamiento sin reclamar locales en el host ESXi.

Etiquetar dispositivos de almacenamiento para vSAN Direct

vSAN Direct necesita algunos discos sin reclamar en cada host ESXi dentro de un clúster de vSAN. Sin embargo, en ciertos entornos, vSAN reclama automáticamente todos los dispositivos de almacenamiento local de los hosts. Puede hacer que los dispositivos no sean aptos para las instancias de vSAN habituales y estén disponibles para vSAN Direct.

Utilice el comando `esxcli` para marcar los dispositivos como vSAN Direct.

Procedimiento

1 Etiquete el dispositivo de almacenamiento local para vSAN Direct.

    `esxcli vsan storage tag add -d` *`diskName`* `-t vsanDirect`

    Por ejemplo:

    `esxcli vsan storage tag add -d mpx.vmhba0:C0:T1:L0 -t vsanDirect`

    El dispositivo dejará de ser apto para la instancia de vSAN regular.

2 Elimine la etiqueta vSAN Direct del dispositivo.

    `esxcli vsan storage tag remove -d` *`diskName`* `-t vsanDirect`

    Por ejemplo:

    `esxcli vsan storage tag remove -d mpx.vmhba0:C0:T1:L0 -t vsanDirect`

Utilizar un script para etiquetar dispositivos de almacenamiento para vSAN Direct

Como alternativa, puede utilizar el siguiente script para etiquetar los dispositivos HDD conectados al host ESXi. Después de ejecutar el script, los dispositivos dejarán de ser aptos para la instancia de vSAN regular y estarán disponibles para vSAN Direct.

```
#!/usr/bin/env python3

# Copyright 2020 VMware, Inc. All rights reserved.

# Abstract
#
#    This script helps manage tagging of Direct Attached HDD disks
#    on ESXi systems for vSAN Direct in preparation for a VCF deployment.
#
```

```
#    It is expected to be used with ESX systems of version 7.0.1 or later.
#

import argparse
from enum import Enum
import logging
import sys
import os
import paramiko
import subprocess
import traceback
import ast
import getpass
from six.moves import input
from distutils.util import strtobool
from argparse import ArgumentParser

class ParseState(Enum):
        OPEN = 0
        DEVICE = 1

class RemoteOperationError(Exception):
    pass

class EsxVersion:

    def __init__(self, major, minor, release):
        self.major = major
        self.minor = minor
        self.release = release

    def __str__(self):
        return '{}.{}.{}'.format(self.major, self.minor, self.release)

    @staticmethod
    def build(str):
        tokens = str.split(b'.',3)
        return EsxVersion(int(tokens[0]), int(tokens[1]), int(tokens[2]))

class StorageDevice:

    def __init__(self, deviceId, isSSD, isVsanDirectEnabled):
        self.deviceId = str(deviceId.decode())
        self.isSSD = isSSD
        self.isVsanDirectCapable = True
        self.isVsanDirectEnabled = isVsanDirectEnabled

    def __str__(self):
        return '{}:\n\tIs SSD: {}\n\tvsanDirect enabled:{}'.format(
                    self.deviceId,
                    self.isSSD,
                    self.isVsanDirectEnabled)

    @staticmethod
    def strToBool(v):
```

```
        return bool(strtobool(str(v.decode())))

    @staticmethod
    def build(deviceId, props):
        vsanDirectEnabled = False
        isLocal = StorageDevice.strToBool(props[b'Is Local'])
        status = props[b'Status']
        isOffline = StorageDevice.strToBool(props[b'Is Offline'])
        isSSD = StorageDevice.strToBool(props[b'Is SSD'])
        isBootDevice = StorageDevice.strToBool(props[b'Is Boot Device'])
        deviceType = props[b'Device Type']
        if deviceType == b'Direct-Access' and isLocal and (not isOffline) and (not 
isBootDevice) and status == b'on':
            return StorageDevice(deviceId, isSSD, vsanDirectEnabled)
        else:
            print("Skipping device {}".format(deviceId))
            return None

def parse_arguments():
    """
    Parses the command line arguments to the function
    """
    parser = argparse.ArgumentParser()
    parser.add_argument('--hostname', dest='hostname',
            help='specify hostname for the ESX Server', required=True)
    parser.add_argument('--username', dest='username',
            help='specify username to connect to the ESX Server', required=True)
    parser.add_argument('--password', dest='password',
            help='specify password to connect to the ESX Server', required=False)
    return parser.parse_args()

def get_esx_version(sshClient):
    global logger
    stdin_, stdout_, stderr_ = sshClient.exec_command('vmware -v')
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to determine ESX version')
    output = stdout_.read()
    tokens = output.split()
    if len(tokens) < 3:
        raise RemoteOperationError('Invalid ESX Version - %s', output)
    return EsxVersion.build(tokens[2])

def check_esx_version(esxVersion):
    return esxVersion.major >= 7 and esxVersion.minor >= 0 and esxVersion.release >= 1

def query_devices(sshClient):
    global logger
    stdin_, stdout_, stderr_ = sshClient.exec_command('esxcli storage core device list')
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
```

```
        raise RemoteOperationError('Failed to query core storage device list')
    output = stdout_.read()
    # Build the device list from the output
    return create_device_list(output)

def create_device_list(str):
    devices = []

    deviceId=""
    deviceProps={}

    parseState = ParseState.OPEN
    for line in str.splitlines():
        if parseState == ParseState.OPEN:
            if line.strip():
                deviceId=line.strip()
                parseState = ParseState.DEVICE
        elif parseState == ParseState.DEVICE:
            if line.strip():
                props = line.strip().split(b':',1)
                deviceProps[props[0]] = props[1].strip()
            else:
                if deviceId:
                    device = StorageDevice.build(deviceId, deviceProps)
                    if device:
                        devices.append(device)
                    else:
                        logger.debug("Skipping device {}".format(deviceId))
                deviceId=""
                deviceProps={}
                parseState = ParseState.OPEN
    if deviceId:
        device = StorageDevice.build(deviceId, deviceProps)
        if device:
            devices.append(device)
    return devices

def tag_device_for_vsan_direct(sshClient, deviceId):
    global logger
    logger.info("Tagging device [{}] for vSAN Direct".format(deviceId))
    command = "esxcli vsan storage tag add -d " + deviceId + " -t vsanDirect"
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to tag device [{}] for vSAN
Direct'.format(deviceId))
    logger.info('Successfully tagged device [{}] for vSAN Direct'.format(deviceId))

def untag_device_for_vsan_direct(sshClient, deviceId):
    global logger
    logger.info("Untagging device [{}] for vSAN Direct".format(deviceId))
    command = "esxcli vsan storage tag remove -d " + deviceId + " -t vsanDirect"
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
```

```
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to untag device [{}] for vSAN 
Direct'.format(deviceId))
    logger.info('Successfully untagged device [{}] for vSAN Direct'.format(deviceId))

def get_vsan_info_for_device(sshClient, deviceId):
    global logger
    command = "vdq -q -d {}".format(deviceId)
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to query vsan direct status on device [%s]' % 
deviceId)
    output = stdout_.read()
    return ast.literal_eval(str(output.decode()))

def update_vsan_direct_status(sshClient, devices):
        for device in devices:
            vsanInfo = get_vsan_info_for_device(sshClient, device.deviceId)
            device.isVsanDirectEnabled = vsanInfo[0]['IsVsanDirectDisk'].strip() == "1"
            device.isVsanDirectCapable = vsanInfo[0]['State'].strip() == 'Eligible for use by 
VSAN'

def getVsanDirectCapableDevices(devices):
    selectDevices = []
    # Cull devices incapable of vSAN Direct
    for device in devices:
        if device.isVsanDirectCapable:
            selectDevices.append(device)
    return selectDevices

def print_devices(devices):
    print("Direct-Attach Devices:")
    print("=====================")
    iDevice = 0
    for device in devices:
        iDevice = iDevice + 1
        print ("{}. {}".format(iDevice, device))
    print("=====================")

def tag_devices(sshClient, devices):
    for device in devices:
        tag_device_for_vsan_direct(sshClient, device.deviceId)

def untag_devices(sshClient, devices):
    for device in devices:
        untag_device_for_vsan_direct(sshClient, device.deviceId)

def tag_all_hdd_devices(sshClient, devices):
    hddDevices = []
```

```
    for device in devices:
        if not device.isSSD:
            hddDevices.append(device)
    if len(hddDevices) > 0:
        tag_devices(sshClient, hddDevices)

def show_usage():
    print ("===================================")
    print ("commands: {tag-all-hdd, tag, untag}")
    print ("\ttag <comma separated serial numbers of devices>")
    print ("\tuntag <comma separated serial numbers of devices>")
    print ("\ttag-all-hdd")
    print ("=============")

def main():
    global logger
    logger.info('Tag disks for vSAN Direct')

    try:
        # Parse arguments
        args = parse_arguments()

        # 1. Setup SSH connection to ESX system
        sshClient = paramiko.SSHClient()
        sshClient.load_system_host_keys()
        sshClient.set_missing_host_key_policy(paramiko.AutoAddPolicy())
        passwd = args.password
        if passwd == None:
            passwd = getpass.getpass(prompt='Password: ')
        logger.info('Connecting to ESX System (IP: %s)' % args.hostname)
        sshClient.connect(args.hostname, username=args.username, password=passwd)
        # version check
        esxVersion = get_esx_version(sshClient)
        print('ESX Version on {} is {}'.format(args.hostname, esxVersion))
        logger.info('Checking ESX Version...')
        if not check_esx_version(esxVersion):
            raise Exception('ESX Version must be 7.0.1 or greater')

        print ('This script helps tag direct-attached disks for vSAN Direct on ESX')
        print ('Note: Only disks of type HDD are supported at this time.')
        print ()
        print ("For help, type help")
        show_usage()

        while True:
            # get device list
            print("Querying devices...")
            devices = query_devices(sshClient)
            # update devices with vSAN Direct status
            update_vsan_direct_status(sshClient, devices)
            # cull device list
            selectDevices = getVsanDirectCapableDevices(devices)
            # List the devices for the user to see
            print_devices(selectDevices)
            # find out what the user wants to do to these devices
```

```
            args = input('Command> ').split()
            if len(args) == 0:
                break
            cmd = args[0]
            if cmd == 'q' or cmd == 'quit' or cmd == 'exit':
                break
            elif cmd == 'help':
                show_usage()
            elif cmd == 'tag-all-hdd':
                print("Tagging all HDD devices...")
                tag_all_hdd_devices(sshClient, selectDevices)
            elif cmd == 'tag' or cmd == 'untag':
                chosenDevices = []
                if len(args) > 1:
                    serials = args[1].split(',')
                    for serialStr in serials:
                        serial = int(serialStr)
                        if serial < 1 or serial > len(selectDevices):
                            raise Exception("Error: Serial {} is out of range".format(serial))
                        chosenDevices.append(selectDevices[serial-1])
                if len(chosenDevices) == 0:
                    print("No devices specified")
                    continue
                if cmd == 'tag':
                    print("Tagging devices...")
                    tag_devices(sshClient, chosenDevices)
                else:
                    print("Untagging devices...")
                    untag_devices(sshClient, chosenDevices)
            else:
                print ("Error: Unrecognized command - %s" % cmd)
    except paramiko.ssh_exception.AuthenticationException as e:
        logger.error(e)
        sys.exit(5)
    except Exception as e:
        logger.error('Disk tagging failed with error: %s' % e)
        logger.error(traceback.format_exc())
        sys.exit(1)
    finally:
        # Close SSH client
        try:
            sshClient.close()
        except:
            pass

# Set up logging
logging.basicConfig()
logger = logging.getLogger('tag-disks-for-vsan-direct')

if __name__ == "__main__":
    main()
```

Crear un almacén de datos de vSAN Direct

Como administrador de vSphere, configure un almacén de datos de vSAN Direct para utilizarlo con funcionalidades como la plataforma de persistencia de datos de vSAN o el almacenamiento de instancias de máquina virtual. Para crear el almacén de datos, use dispositivos de almacenamiento sin reclamar que estén en el host ESXi.

Puede crear el almacén de datos de vSAN Direct cuando habilite vSAN para el Supervisor. La siguiente tarea muestra cómo se reclaman dispositivos de almacenamiento local como vSAN Direct cuando vSAN ya está habilitado en el clúster.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

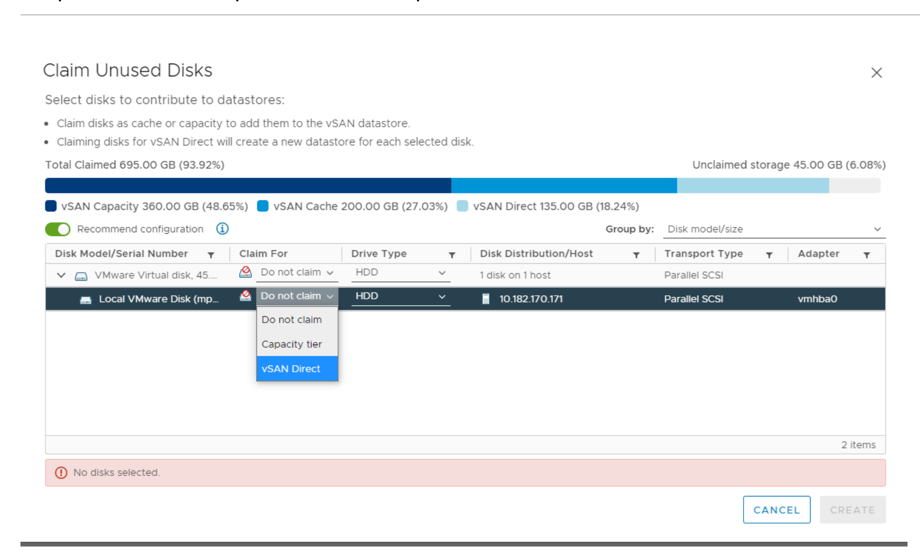
3 En vSAN, haga clic en **Administración de discos**.

4 Haga clic en **Reclamar discos sin utilizar**.

5 En el cuadro de diálogo **Reclamar discos sin utilizar**, haga clic en la pestaña **vSAN Direct**.

6 Seleccione un dispositivo para reclamar y seleccione una casilla de verificación en la columna **Reclamar para vSAN Direct** .

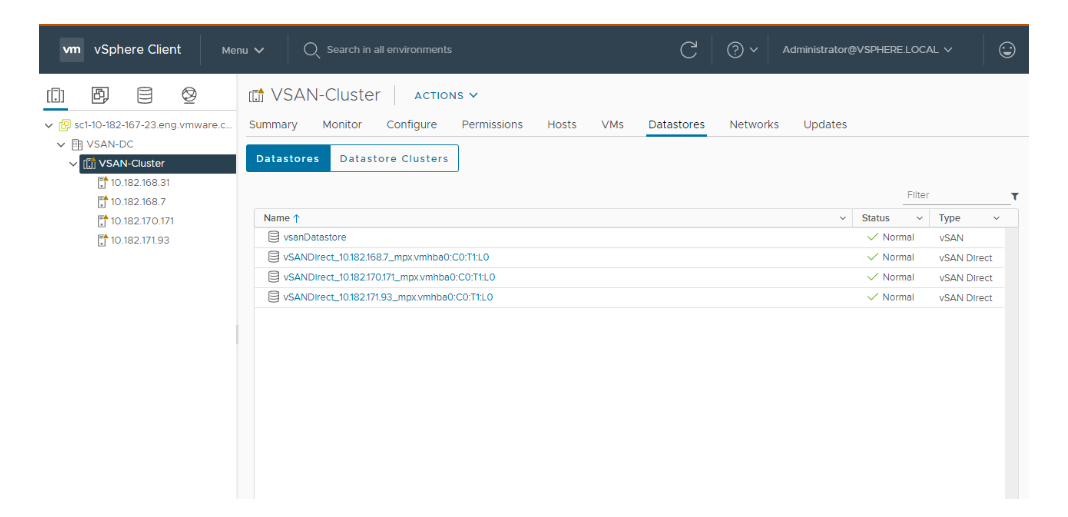
Nota Si reclamó los dispositivos para un almacén de datos de vSAN normal, estos dispositivos no aparecen en la pestaña **vSAN Direct** .



7 Haga clic en **Crear**.

En cada dispositivo que reclame, vSAN Direct crea un almacén de datos nuevo.

8 Haga clic en la pestaña **Almacenes de datos** para mostrar todos los almacenes de datos de vSAN Direct en el clúster.



Pasos siguientes

Puede utilizar vSAN Direct con almacenamiento externo. Para obtener más información, consulte Usar el almacenamiento externo con vSAN Direct en la documentación de *Mantenimiento del plano de control de IaaS de vSphere*.

Supervisar servicios con estado en vSphere IaaS control plane

Después de habilitar los servicios con estado integrados de terceros, utilice las funciones de supervisión de capacidad y estado de vSAN para ver el estado y analizar el uso que hacen del espacio los objetos de servicio.

Procedimiento

1 En vSphere Client, desplácese hasta Supervisor.

2 Haga clic en la pestaña **Supervisar**.

3 Supervise los objetos virtuales que se ejecutan en el espacio de nombres que corresponde al servicio habilitado.

   a En **vSAN**, haga clic en **Objetos virtuales**.

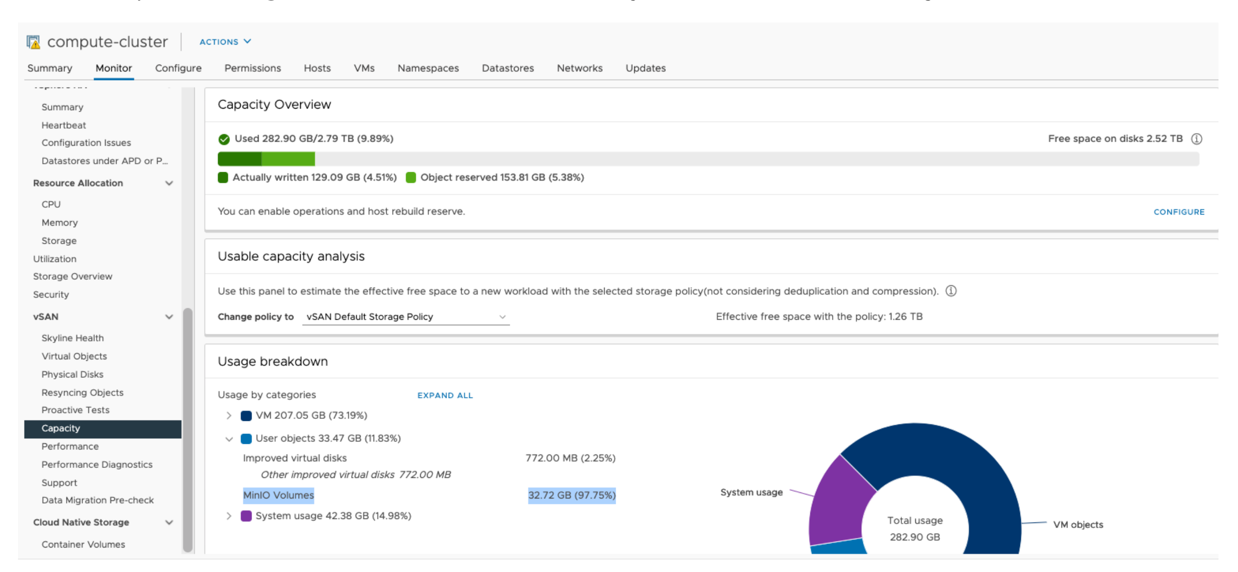
      Puede examinar los objetos virtuales, como los objetos del operador de MinIO, y comprobar su estado.

   b Para ver la colocación del objeto en toda la infraestructura física, seleccione un objeto concreto y haga clic en **VER DETALLES DE COLOCACIÓN**.

4 Supervise la capacidad que utilizan los objetos de servicio.

   a En **vSAN**, haga clic en **Capacidad**.

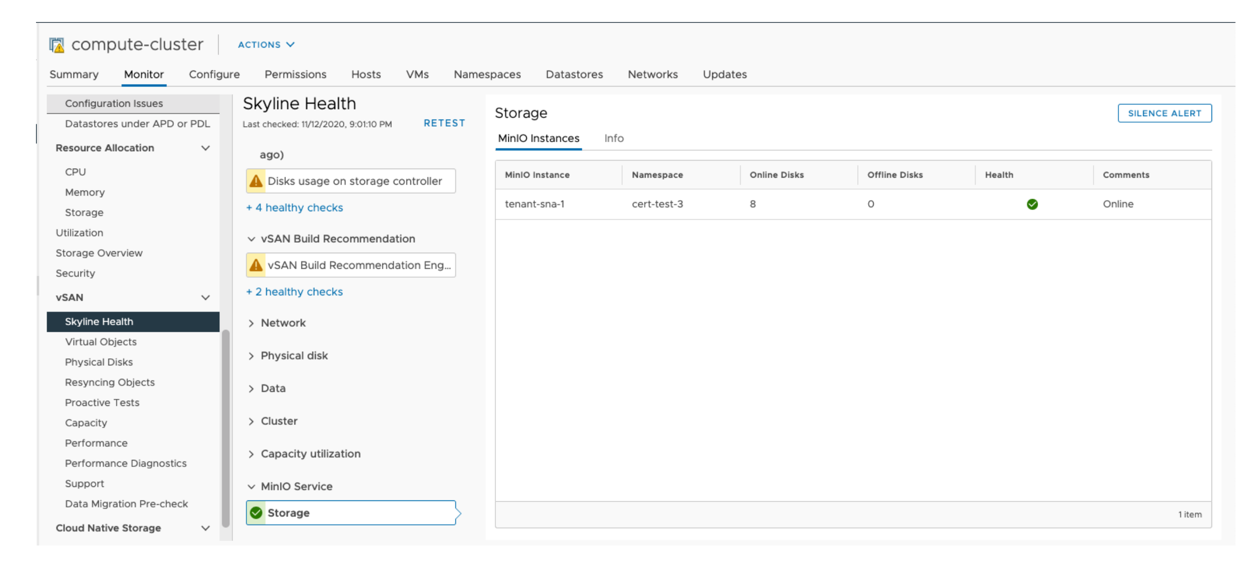
   b En el panel **Desglose de uso**, muestre los objetos de servicio en **Objetos de usuario**.



5 Supervise el estado de las instancias del servicio.

   a En **vSAN**, seleccione **Skyline Health**.

   b Seleccione una comprobación de estado de servicio individual para ver la información detallada.



Comprobar las directivas de almacenamiento disponibles para los servicios con estado

Como ingeniero de desarrollo y operaciones, compruebe que el espacio de nombres que utiliza para los servicios con estado en el entorno vSphere IaaS control plane tenga las clases

de almacenamiento adecuadas. Las clases de almacenamiento pueden ser Shared-Nothing-Architecture (SNA) de vSAN y vSAN Direct.

La plataforma persistencia de datos de vSAN crea automáticamente estas clases de almacenamiento en el espacio de nombres después de que un administrador de vSphere habilite el servicio con estado. Consulte Habilitar servicios con estado en vSphere IaaS control plane.

Nota Solo las aplicaciones que se ejecutan en el Supervisor pueden utilizar las clases de almacenamiento vsan-direct y vsan-sna. Estas clases de almacenamiento no se pueden utilizar dentro de un clúster de Tanzu Kubernetes Grid.

Además de las clases de almacenamiento predeterminadas, el administrador de vSphere también puede crear directivas de almacenamiento personalizadas y asignarlas al espacio de nombres. Consulte Crear directiva de almacenamiento de vSAN Direct y Crear directiva de almacenamiento SNA vSAN.

Procedimiento

- Compruebe que las directivas de almacenamiento que se usarán con vSAN SNA y vSAN Direct estén disponibles en el espacio de nombres.

```
# kubectl get sc
NAME                        PROVISIONER               RECLAIMPOLICY   VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION   AGE
sample-vsan-direct-thick    csi.vsphere.vmware.com    Delete          WaitForFirstConsumer
true                   3m36s
sample-vsan-sna-thick       csi.vsphere.vmware.com    Delete          WaitForFirstConsumer
true                   13m
```

Crear directivas de almacenamiento personalizadas para la plataforma de persistencia de datos de vSAN

Cuando se habilita un servicio con estado en un Supervisor de vSphere IaaS control plane, la plataforma de persistencia de datos de vSAN crea directivas de almacenamiento predeterminadas y las clases de almacenamiento correspondientes, y las asigna al espacio de nombres del servicio. Las directivas son para almacenes de datos de vSAN Shared-Nothing-Architecture (SNA) y vSAN Direct. En lugar de la predeterminada, puede crear directivas de almacenamiento personalizadas.

Para decidir qué tipo de almacén de datos se debe utilizar, siga estas recomendaciones generales:

- Use vSAN Direct, en cambio, si va a crear un clúster de hardware dedicado para los servicios nativos en la nube que no comparten nada.

- Utilice vSAN con SNA cuando quiera que la aplicación con estado nativa en la nube comparta la infraestructura física con otras máquinas virtuales comunes o con cargas de trabajo de Kubernetes. Cada carga de trabajo puede definir su propia directiva de almacenamiento y puede obtener lo mejor de ambos mundos desde un solo clúster.

Para obtener más información, consulte Almacenamiento que no comparte nada de vSphere.

Después de crear la directiva, puede asignarla al espacio de nombres donde se ejecuta el servicio con estado. Consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.

Crear directiva de almacenamiento de vSAN Direct

Si utiliza vSAN Direct, cree una directiva de almacenamiento que se utilizará con un espacio de nombres de Supervisor. En el espacio de nombres que se asocia con esta directiva de almacenamiento, se pueden ejecutar cargas de trabajo compatibles con vSAN Direct, por ejemplo, servicios con estado o máquinas virtuales de almacenamiento de instancia.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a En el menú **Inicio**, haga clic en **Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva**, en **Reglas específicas de almacenes de datos**, habilite las reglas para la colocación del almacenamiento de vSAN Direct.

4 En la página **Reglas de vSAN Direct**, especifique vSAN Direct como un tipo de colocación de almacenamiento.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos de vSAN Direct que coinciden con esta directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Crear directiva de almacenamiento SNA vSAN

Si utiliza vSAN con una plataforma persistencia de datos de vSAN, puede crear una directiva de almacenamiento de arquitectura de no compartir nada (SNA) vSAN para usarla con el espacio de nombres donde se ejecutan los servicios con estado.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a En el menú **Inicio**, haga clic en **Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento, por ejemplo, **`Ejemplo de SNA grueso`**.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva**, en **Reglas específicas de almacenes de datos**, habilite las reglas para la colocación del almacenamiento de vSAN.

4 En la página **vSAN**, haga clic en la pestaña **Disponibilidad** y seleccione los siguientes valores. Los valores solo se aplican a las cargas de trabajo de SNA en la plataforma persistencia de datos de vSAN. No se pueden utilizar para aprovisionar cargas de trabajo de máquinas virtuales.

Opción	Descripción
Opción	Valor
Tolerancia de desastres en el sitio	**Ninguno: clúster estándar** **Nota** La plataforma persistencia de datos de vSAN solo admite clústeres estándares.
Errores que se toleran	**No hay redundancia de datos con afinidad de host**

   Aprovisionamiento grueso aplicado para las cargas de trabajo de SNA y se selecciona como un valor para la reserva de espacio de objetos en la pestaña **Reglas de directivas avanzadas**. No puede cambiar este valor.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos de vSAN que coinciden con esta directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

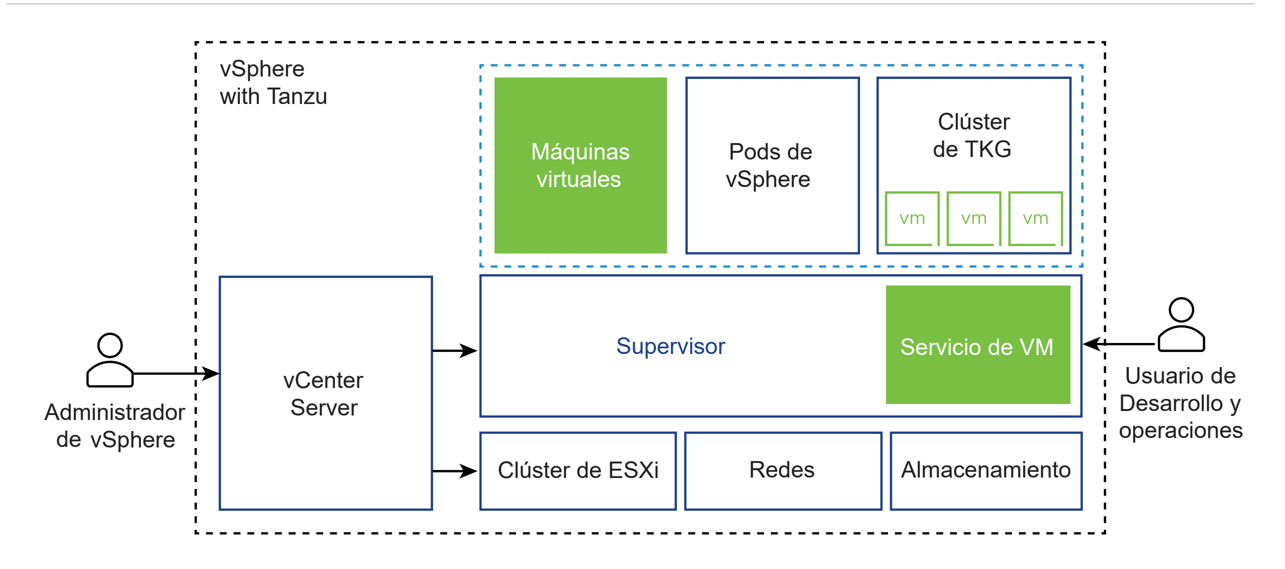
Implementar y administrar máquinas virtuales en vSphere IaaS control plane

6

vSphere IaaS control plane ofrece una funcionalidad de servicio de máquina virtual que permite a los ingenieros de desarrollo y operaciones implementar y ejecutar máquinas virtuales, además de contenedores, en un entorno de Kubernetes común y compartido. Puede utilizar el servicio de máquina virtual para administrar el ciclo de vida de las máquinas virtuales en un espacio de nombres. El servicio de máquina virtual administra las máquinas virtuales independientes y las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes Grid.

El servicio de máquina virtual responde a las necesidades de los equipos de desarrollo y operaciones que usan Kubernetes, pero tienen cargas de trabajo basadas en máquinas virtuales existentes que no se pueden colocar en contenedores fácilmente. También ayuda a los usuarios a reducir la sobrecarga de administrar una plataforma que no es de Kubernetes junto con una plataforma de contenedor. Al ejecutar contenedores y máquinas virtuales en una plataforma de Kubernetes, los equipos de desarrollo y operaciones pueden consolidar su marca de carga de trabajo en una sola plataforma.

Nota Además de las máquinas virtuales independientes, el servicio de máquina virtual administra las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes Grid. Para obtener información acerca de los clústeres, consulte la documentación de *Uso del servicio TKG con el plano de control de IaaS de vSphere*.



Cada máquina virtual implementada a través del servicio de máquina virtual funciona como una máquina completa que ejecuta todos los componentes, incluido su propio sistema operativo, sobre la infraestructura de vSphere IaaS control plane. La máquina virtual tiene acceso a las redes y al almacenamiento que proporciona Supervisor, y se administra mediante el comando estándar `kubectl` de Kubernetes. La máquina virtual se ejecuta como un sistema completamente aislado que está a prueba de interferencias de otras máquinas virtuales o cargas de trabajo en el entorno de Kubernetes.

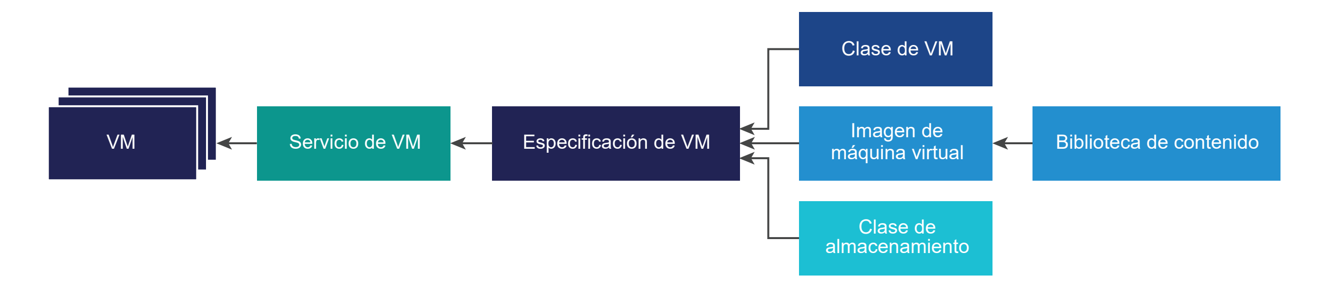
¿Cuándo utilizar máquinas virtuales en una plataforma de Kubernetes?

Por lo general, la decisión de ejecutar cargas de trabajo en un contenedor o en una máquina virtual depende de sus necesidades y objetivos empresariales. Entre los motivos para utilizar las máquinas virtuales aparecen los siguientes:

- Las aplicaciones no se pueden poner en contenedores.
- Tiene requisitos de hardware específicos para el proyecto.
- Las aplicaciones están diseñadas para un kernel personalizado o un sistema operativo personalizado.
- Las aplicaciones son más adecuadas para ejecutarse en una máquina virtual.
- Desea tener una experiencia de Kubernetes coherente y evitar la sobrecarga. En lugar de ejecutar conjuntos separados de infraestructura para las plataformas de contenedor y que no son de Kubernetes, puede consolidar estas pilas y administrarlas con un comando de `kubectl` familiar.

Conceptos del servicio de máquina virtual

Para describir el estado de una máquina virtual que se implementará en un espacio de nombres de vSphere, utilice parámetros como una clase de máquina virtual, una imagen de máquina virtual y una clase de almacenamiento. A continuación, el servicio de máquina virtual reúne estas especificaciones para crear máquinas virtuales independientes o máquinas virtuales que admitan clústeres de Tanzu Kubernetes Grid.



Servicio de VM

El servicio de máquina virtual es un componente de vSphere IaaS control plane que proporciona una API declarativa de tipo Kubernetes para la administración de las máquinas virtuales y los recursos de vSphere asociados. El servicio de máquina virtual permite a los administradores de vSphere entregar recursos y proporcionar plantillas, como clases e imágenes de máquinas virtuales, a Kubernetes. Los ingenieros de desarrollo y operaciones pueden utilizar estos recursos para describir el estado deseado de una máquina virtual. Después de que los ingenieros de desarrollo y operaciones especifiquen el estado de la máquina virtual, el servicio de máquina virtual convierte el estado deseado en un estado realizado en función de los recursos de la infraestructura de respaldo.

Una máquina virtual creada a través del servicio de máquina virtual solo se puede administrar desde el espacio de nombres de Kubernetes con los comandos de `kubectl`. Los administradores de vSphere no pueden administrar la máquina virtual desde vSphere Client, pero pueden mostrar sus detalles y supervisar los recursos que utiliza. Para obtener información, consulte Supervisar máquinas virtuales disponibles en vSphere IaaS control plane.

Clase de VM

La clase de máquina virtual es una especificación de máquina virtual que se puede utilizar para solicitar un conjunto de recursos para una máquina virtual. La clase de máquina virtual es controlada y administrada por un administrador de vSphere, y define parámetros como el número de CPU virtuales, la capacidad de memoria y la configuración de reserva. Los parámetros definidos están avalados y garantizados por los recursos de infraestructura subyacentes de un Supervisor.

Un administrador de vSphere puede crear clases de máquinas virtuales personalizadas.

Además, la administración de cargas de trabajo ofrece varias clases de máquinas virtuales predeterminadas. Por lo general, cada tipo de clase predeterminada viene en dos ediciones: garantizada y de mejor esfuerzo. Una edición garantizada reserva por completo los recursos que solicita una especificación de máquina virtual. Una edición de clase de mejor esfuerzo no lo hace, y permite que los recursos se sobreasignen. Por lo general, en un entorno de producción, se utiliza un tipo garantizado.

A continuación, se muestran ejemplos de clases de máquinas virtuales predeterminadas.

Clase	CPU	Memoria (GB)	CPU y memoria reservadas
`guaranteed-large`	4	16	Sí
`best-effort-large`	4	16	No
`guaranteed-small`	2	4	Sí
`best-effort-small`	2	4	No

vSphere puede asignar cualquier cantidad de clases de máquinas virtuales existentes para que estén disponibles para los ingenieros de desarrollo y operaciones en un espacio de nombres específico.

La clase de máquina virtual proporciona una experiencia simplificada para los ingenieros de desarrollo y operaciones. Estos no necesitan comprender la configuración completa de cada máquina virtual que planean crear. En su lugar, pueden seleccionar una clase de máquina virtual entre las opciones disponibles, y el servicio de máquina virtual administra la configuración de la máquina virtual.

En el lado de Kubernetes, las clases de máquinas virtuales aparecen como recursos `VirtualMachineClass`.

Imagen de máquina virtual

Una imagen de máquina virtual es una plantilla que contiene una configuración de software, que incluye un sistema operativo, aplicaciones y datos.

Cuando los ingenieros de desarrollo y operaciones crean máquinas virtuales, pueden seleccionar imágenes de la biblioteca de contenido asociada con el espacio de nombres. En desarrollo y operaciones, las imágenes se exponen como objetos de `VirtualMachineImage`.

Un administrador de vSphere puede crear imágenes de máquina virtual que sean compatibles con vSphere IaaS control plane y cargarlas en una biblioteca de contenido.

Biblioteca de contenido

Un ingeniero de desarrollo y operaciones utiliza una biblioteca de contenido como origen de las imágenes para crear una máquina virtual. De forma similar a las clases de máquina virtual, un administrador de vSphere asigna bibliotecas de contenido existentes a un espacio de nombres o a un clúster para que estén disponibles para los ingenieros de desarrollo y operaciones. El administrador de vSphere también puede hacer que se pueda escribir en la biblioteca de contenido del espacio de nombres. Este permiso adicional permite a los usuarios de desarrollo y operaciones publicar sus imágenes en la biblioteca.

Clase de almacenamiento

El servicio de máquina virtual utiliza clases de almacenamiento para colocar discos virtuales y asociar volúmenes persistentes de forma dinámica. Para obtener más información sobre las clases de almacenamiento, consulte Capítulo 8 Usar almacenamiento persistente con cargas de trabajo de Supervisor en vSphere IaaS control plane.

Especificación de la máquina virtual

Los ingenieros de desarrollo y operaciones describen el estado deseado de una máquina virtual en un archivo YAML que une la imagen de la máquina virtual, la clase de máquina virtual y la clase de almacenamiento.

Operador de máquina virtual para Kubernetes

El operador de máquina virtual permite la administración de máquinas virtuales con una API declarativa de estilo Kubernetes.

A partir de vSphere 8.0 Update 3, vSphere IaaS control plane admite el operador de máquina virtual v1alpha2. Entre otras ventajas, esta versión ofrece las siguientes capacidades:

- Compatibilidad mejorada con proveedores de arranque, incluida la compatibilidad con Cloud-Init y Windows en línea.
- Configuración mejorada de redes invitadas.
- Capacidades de estado aumentadas.
- Compatibilidad con puertas de preparación definidas por el usuario.
- Nueva API de VirtualMachineWebConsoleRequest.

Además de los nuevos cambios de API específicos de v1alpha2, la mayoría de las otras API de v1alpha2 pueden funcionar en paridad con v1alpha1. La mayoría de los campos de las especificaciones de máquina virtual son compatibles con versiones anteriores de v1alpha1.

Después de la publicación de v1alpha2, puede seguir usando los objetos v1alpha1. Todos los objetos v1alpha1 se convertirán automáticamente a v1alpha2 mediante webhooks de conversión integrados en el operador de máquina virtual.

Para obtener información sobre el operador de máquina virtual v1alpha2 y los campos compatibles, consulte https://vm-operator.readthedocs.io/en/stable/ref/api/v1alpha2/.

Redes

El servicio de máquina virtual no tiene ningún requisito específico y se basa en la configuración de red disponible en vSphere IaaS control plane. El servicio de máquina virtual admite ambos tipos de redes, las redes de vSphere o NSX. Cuando se implementan máquinas virtuales, un proveedor de red disponible asigna direcciones IP estáticas a las máquinas virtuales. Para obtener más información, consulte Redes de supervisor en la documentación de *Planificación y conceptos del plano de control de IaaS de vSphere*.

Servicio de máquina virtual y Supervisor con zonas de vSphere

Cuando se crean máquinas virtuales en un Supervisor de tres zonas, la instancia de máquina virtual se replica en todas las zonas disponibles. Para controlar la colocación de las máquinas virtuales a través del archivo YAML, el equipo de desarrollo y operaciones puede utilizar la etiqueta de Kubernetes `topology.kubernetes.io/zone`. Por ejemplo, `topology.kubernetes.io/zone: zone-a02`.

Flujo de trabajo para aprovisionar y supervisar una máquina virtual

Como administrador de vSphere, debe establecer barreras para la directiva y el gobierno de las máquinas virtuales, y entregar recursos de máquina virtual, como clases de máquinas virtuales y plantillas de máquina virtual, a los ingenieros de desarrollo y operaciones. Después de implementar una máquina virtual, puede supervisarla mediante vSphere Client.

Paso	Realizado por	Descripción
1	Administrador de vSphere	Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere IaaS control plane
2	Administrador de vSphere	Trabajar con clases de máquinas virtuales en vSphere IaaS control plane Para usar la vGPU de NVIDIA, configure un dispositivo PCI en la clase de máquina virtual. Consulte Implementar una máquina virtual con vGPU y otros dispositivos PCI en vSphere IaaS control plane.
3	Ingeniero de desarrollo y operaciones	Implementar una máquina virtual independiente en vSphere IaaS control plane Para las máquinas virtuales del clúster de Tanzu Kubernetes Grid, consulte *Uso del servicio TKG con el plano de control de IaaS de vSphere*.
4	Administrador de vSphere	Supervisar máquinas virtuales disponibles en vSphere IaaS control plane
5	Ingeniero de desarrollo y operaciones	Administrar y publicar imágenes de la biblioteca de contenido en vSphere IaaS control plane

Lea los siguientes temas a continuación:

- Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere IaaS control plane
- Trabajar con clases de máquinas virtuales en vSphere IaaS control plane
- Crear y administrar clases de máquina virtual mediante la CLI del centro de datos
- Implementar una máquina virtual independiente en vSphere IaaS control plane
- Implementar una máquina virtual con vGPU y otros dispositivos PCI en vSphere IaaS control plane
- Implementar una máquina virtual con almacenamiento de instancias en vSphere IaaS control plane
- Implementar máquinas virtuales con propiedades OVF configurables en vSphere IaaS control plane
- Supervisar máquinas virtuales disponibles en vSphere IaaS control plane
- Solucionar problemas de máquinas virtuales mediante la consola web de máquina virtual de vSphere

Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere IaaS control plane

Para implementar máquinas virtuales en el entorno de vSphere IaaS control plane, los usuarios de desarrollo y operaciones deben tener acceso a imágenes de máquina virtual, o plantillas, que contengan configuraciones de software, incluidos sistemas operativos, aplicaciones y datos. Para proporcionar acceso a imágenes, un administrador de vSphere configura una biblioteca de contenido de máquina virtual y la asocia con el espacio de nombres donde se implementan las máquinas virtuales. A partir de vSphere 8.0 Update 2, el administrador de vSphere también puede asignar la biblioteca de contenido en un nivel de Supervisor a fin de que esté disponible para todos los espacios de nombres.

Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere IaaS control plane

Como administrador de vSphere, cree una biblioteca de contenido para almacenar y administrar plantillas de máquina virtual.

Crear una biblioteca de contenido para máquinas virtuales independientes

Puede crear una biblioteca de contenido local y rellenarla con plantillas y otros tipos de archivos. También puede crear una biblioteca suscrita para utilizar el contenido de una biblioteca local publicada ya existente.

Para proteger los elementos de una biblioteca de contenido, puede aplicar una directiva de seguridad de OVF. La directiva de seguridad de OVF aplica una validación estricta al implementar o actualizar una biblioteca de contenido, importar elementos a una biblioteca de contenido o sincronizar plantillas. Para asegurarse de que las plantillas estén firmadas por un certificado de confianza, puede agregar el certificado de firma de OVF desde una entidad de certificación de confianza en una biblioteca de contenido.

Para obtener más información sobre las bibliotecas de contenido y las plantillas de máquina virtual de vSphere, consulte Usar bibliotecas de contenido en *Administrar máquinas virtuales de vSphere*.

Requisitos previos

Privilegios necesarios:

- **Biblioteca de contenido.Crear biblioteca local** o **Biblioteca de contenido.Crear biblioteca suscrita** en la instancia de vCenter Server en la que desea crear la biblioteca.
- **Almacén de datos.Asignar espacio** en el almacén de datos de destino.

Procedimiento

1 Desplácese a la página **Servicio de máquina virtual**.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en la tarjeta **Servicio de máquina virtual**.

2 En la página **Servicio de máquina virtual**, haga clic en **Bibliotecas de contenido > Crear una biblioteca de contenido**.

   Esta acción lo lleva a la sección de la biblioteca de contenido de vSphere Client.

3 Haga clic en **Crear**.

   Se abrirá el asistente **Nueva biblioteca de contenido**.

4 En la página **Nombre y ubicación**, introduzca un nombre, seleccione una instancia de vCenter Server para la biblioteca de contenido y haga clic en **Siguiente**.

   Asegúrese de utilizar un nombre informativo para la biblioteca de contenido, de modo que el equipo de desarrollo y operaciones pueda encontrarlos y acceder a ellos fácilmente.

5 En la página **Configurar biblioteca de contenido**, seleccione el tipo de biblioteca de contenido que desea crear y haga clic en **Siguiente**.

Opción	Descripción
Biblioteca de contenido local	De forma predeterminada, solo se puede acceder a una biblioteca de contenido local en la instancia de vCenter Server en la que se creó. a (opcional) Para que el contenido de la biblioteca esté disponible para otras instancias de vCenter Server, seleccione **Habilitar publicación**. b (opcional) Si desea requerir una contraseña para acceder a la biblioteca de contenido, seleccione **Permitir autenticación** y establezca una contraseña.
Biblioteca de contenido suscrita	Una biblioteca de contenido suscrita se origina en una biblioteca de contenido publicada. Utilice esta opción para aprovechar las bibliotecas de contenido existentes. Es posible sincronizar la biblioteca suscrita con la biblioteca publicada para ver el contenido actualizado, pero no se puede agregar ni quitar contenido de la biblioteca suscrita. Solo un administrador de la biblioteca publicada puede agregar, modificar y quitar contenido de la biblioteca publicada. Proporcione la siguiente información para suscribirse a una biblioteca: a En el cuadro de texto **URL de suscripción**, escriba la dirección URL de la biblioteca publicada. b Si está habilitada la autenticación en la biblioteca publicada, seleccione **Habilitar autenticación** y escriba la contraseña del editor. c Seleccione un método de descarga para el contenido de la biblioteca suscrita. ■ Si desea descargar una copia local de todos los elementos de una biblioteca publicada inmediatamente después de suscribirla, seleccione **inmediatamente**. ■ Si desea ahorrar espacio de almacenamiento, seleccione **solo cuando sea necesario**. Solo se descargan los metadatos para los elementos de la biblioteca publicada. Si necesita utilizar un elemento, sincronice el elemento o la biblioteca completa para descargar su contenido. d Cuando se le pida, acepte la huella digital de certificado SSL. El certificado SSL se almacena en su sistema hasta que la biblioteca de contenido suscrita se elimine del inventario.

6 (opcional) En la página **Aplicar directiva de seguridad**, seleccione **Aplicar directiva de seguridad** y seleccione **Directiva predeterminada de OVF**.

Para la biblioteca suscrita, esta opción aparece solo si la biblioteca admite políticas de seguridad.

Si selecciona esta opción, el sistema realiza una verificación de certificado OVF estricta al importar un elemento de OVF a la biblioteca desde el host local o sincronizar un elemento. No se pueden importar los elementos de OVF que no aprueben la validación del certificado.

Si el elemento no supera la validación durante la sincronización, se marca con la etiqueta **Error en la verificación**. Solo se conservarán el elemento y los metadatos, pero no los archivos del elemento.

7 En la página **Agregar almacenamiento**, seleccione un almacén de datos como ubicación de almacenamiento para el contenido de la biblioteca de contenido y haga clic en **Siguiente**.

8 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

Rellenar una biblioteca de contenido con imágenes de máquina virtual para máquinas virtuales independientes

Después de crear la biblioteca de contenido, rellénela con plantillas de máquina virtual en formato OVA u OVF. Los ingenieros de desarrollo y operaciones pueden utilizar las plantillas para aprovisionar nuevas máquinas virtuales independientes en el entorno de vSphere IaaS control plane.

Puede utilizar varios métodos para rellenar la biblioteca. En este tema se describe cómo puede agregar elementos a una biblioteca de contenido local mediante la importación de archivos del equipo local o desde un servidor web. Para obtener otras maneras de rellenar la biblioteca de contenido, consulte Rellenar bibliotecas con contenido en*Administrar máquinas virtuales de vSphere*.

Nota No hay restricciones en las imágenes de máquina virtual que puede utilizar. Si desea probar las imágenes OVA listas para utilizar, puede descargarlas de la página Imágenes recomendadas. Tenga en cuenta que estas imágenes son solo para uso en la validación técnica. En el entorno de producción, cree imágenes con las revisiones más recientes y la configuración de seguridad requerida que sigan las directivas de seguridad corporativas.

Requisitos previos

- Cree imágenes de máquina virtual que sean compatibles con vSphere IaaS control plane.

  La especificación de imagen requiere que todas las imágenes de máquina virtual incluyan VMware Tools o un paquete de código abierto equivalente. Las imágenes deben utilizar una de las siguientes opciones para arrancar el SO invitado y su pila de redes. Para obtener más información, consulte Proveedores de arranque.

  - Linux + Cloud-Init versión 17.9-21.2 con DataSourceVMwareGuestInfo.
  - + + Cloud-Init versión 21.3+
  - Windows + Cloudbase-Init versión 1.1.0+
  - Windows + Sysprep (preparación del sistema)

  Para obtener información sobre Cloud-Init, consulte la documentación oficial en Estándar para personalizar instancias de nube.

  Para obtener información sobre Sysprep, consulte la documentación oficial en la información general de Sysprep.

- Si la biblioteca está protegida por una directiva de seguridad, asegúrese de que todos los elementos de la biblioteca sean compatibles. Si una biblioteca protegida incluye una combinación de elementos conformes y no conformes, `kubectl get virtualmachineimages` no puede presentar imágenes de máquina virtual a los ingenieros de desarrollo y operaciones.
- Privilegio necesario: **Biblioteca de contenido.Agregar elemento de biblioteca** y **Biblioteca de contenido.Actualizar archivos** en la biblioteca.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Bibliotecas de contenido**.

2 Haga clic con el botón derecho en una biblioteca de contenido local y seleccione **Importar elemento**.

Se abrirá el cuadro de diálogo **Importar elemento de la biblioteca**.

3 En la sección **Origen**, seleccione el origen del elemento.

Opción	Descripción
URL	Introduzca la ruta de acceso al servidor web donde se encuentra el elemento. **Nota** Puede importar un archivo `.ovf` o `.ova`. El elemento de biblioteca de contenido resultante es del tipo de plantilla de OVF.
Archivo local	Haga clic en **Cargar archivo** para desplazarse hasta el archivo que desea importar desde el sistema local. Puede utilizar el menú desplegable para filtrar los archivos en el sistema local. **Nota** Puede importar un archivo `.ovf` o `.ova`. Al importar una plantilla de OVF, en primer lugar seleccione el archivo de descriptor OVF (`.ovf`). A continuación, se le solicitará que seleccione los demás archivos en la plantilla de OVF (por ejemplo, el archivo `.vmdk`). El elemento de biblioteca de contenido resultante es del tipo de plantilla de OVF.

vCenter Server lee y valida los archivos de manifiesto y de certificado en el paquete de OVF durante la importación. Se muestra una advertencia en el asistente **Elemento de biblioteca de importación** si existen problemas con el certificado, por ejemplo, si vCenter Server detecta un certificado caducado.

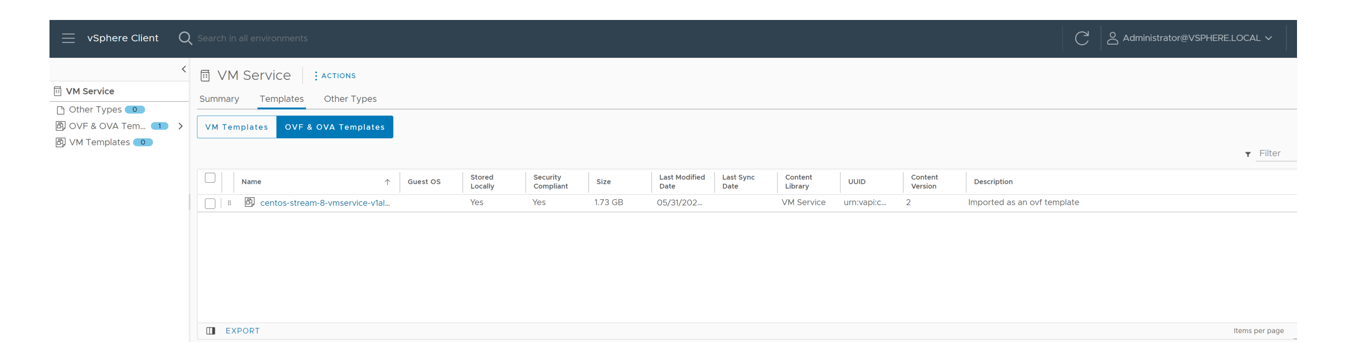
Nota vCenter Server no lee el contenido firmado si se importa el paquete de OVF desde un archivo `.ovf` de la máquina local.

4 En la sección **Destino**, introduzca un nombre y una descripción para el elemento.

5 Haga clic en **Importar**.

Resultados

El elemento aparecerá en la pestaña **Plantillas** o en la pestaña **Otros tipos**.



Agregar y administrar bibliotecas de contenido de máquina virtual en vSphere IaaS control plane

Después de crear la biblioteca de contenido y rellenarla con plantillas de máquina virtual, utilice vSphere Client para agregar la biblioteca al espacio de nombres. Al agregar la biblioteca al espacio de nombres, se otorga a los usuarios de desarrollo y operaciones acceso a la biblioteca. Además, con los comandos de la CLI del centro de datos (DCLI) puede agregar al espacio de nombres una biblioteca de contenido de solo lectura o en la que se pueda escribir, o puede asignar una biblioteca de solo lectura en el nivel del clúster.

Agregar una biblioteca de contenido de máquina virtual a un espacio de nombres mediante vSphere Client

La biblioteca de contenido que se agregue con vSphere Client será de solo lectura. Los usuarios de desarrollo y operaciones podrán acceder a imágenes desde esta biblioteca de contenido, pero no podrán publicar imágenes de máquina virtual en ella.

Puede agregar varias bibliotecas de contenido a un único espacio de nombres. Puede agregar la misma biblioteca de contenido a distintos espacios de nombres.

Nota Este procedimiento se aplica solo a las bibliotecas de contenido para el servicio de máquina virtual. Las bibliotecas de contenido de Tanzu Kubernetes Grid deben administrarse desde la tarjeta de Tanzu Kubernetes Grid.

Requisitos previos

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue una biblioteca de contenido.

a En la tarjeta **Servicio de máquina virtual**, haga clic en **Agregar biblioteca de contenido**.

b Seleccione una o varias bibliotecas de contenido y haga clic en **Aceptar**.

Administrar bibliotecas de contenido de máquina virtual en un espacio de nombres con vSphere Client

Después de asociar la biblioteca con el espacio de nombres, puede usar vSphere Client para eliminarla del espacio de nombres. También puede agregar más bibliotecas.

La eliminación de una biblioteca de contenido de un espacio de nombres no afecta a las máquinas virtuales que se implementaron previamente con las imágenes de la biblioteca.

Nota Este procedimiento se aplica solo a las bibliotecas de contenido para el servicio de máquina virtual. Las bibliotecas de contenido de Tanzu Kubernetes Grid deben administrarse desde la tarjeta de Tanzu Kubernetes Grid.

Requisitos previos

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.

a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue o elimine una biblioteca de contenido.

a En la tarjeta **Servicio de máquina virtual**, haga clic en **Administrar biblioteca de contenido**.

b Realice una de las siguientes operaciones.

Opción	Descripción
Eliminar una biblioteca de contenido	Anule la selección de la biblioteca de contenido y haga clic en **Aceptar**.
Agregar una biblioteca de contenido	Seleccione una o varias bibliotecas de contenido y haga clic en **Aceptar**.

Pasos siguientes

Las plantillas de OVF de la biblioteca se vuelven disponible en el espacio de nombres de Kubernetes como imágenes de máquina virtual. Desarrollo y operaciones puede utilizarlo para

realizar el autoservicio de las máquinas virtuales. Consulte Implementar una máquina virtual en vSphere IaaS control plane.

Nota Solo las plantillas de OVF de la biblioteca se muestran en los espacios de nombres. Otros tipos de contenido no se muestran en el espacio de nombres.

Agregar una biblioteca de contenido de máquina virtual a un espacio de nombres mediante la CLI del centro de datos

Como administrador de vSphere, puede utilizar el comando de la CLI del centro de datos (DCLI, Data Center CLI) para asignar la biblioteca de contenido a un espacio de nombres. Al asignar la biblioteca, puede hacer que se pueda escribir en la biblioteca asociada al espacio de nombres. Cuando se puede escribir en la biblioteca, además de ver la biblioteca y las imágenes que hay en ella, los usuarios de desarrollo y operaciones pueden publicar nuevas imágenes de máquina virtual en ella.

Con los comandos de la DCLI, puede agregar cualquier tipo de biblioteca, ya sea local, publicada y suscrita, al espacio de nombres. Sin embargo, solo podrá escribir en las bibliotecas locales y publicadas que vincule. Las bibliotecas de contenido y los elementos de biblioteca solo están disponibles en el espacio de nombres asociado.

Procedimiento

1 Inicie sesión en vCenter Server con la cuenta de usuario raíz.

2 Escriba `dcli +i` para utilizar la DCLI en modo interactivo.

3 Obtenga el identificador de la biblioteca de contenido que se asociará al espacio de nombres.

   `dcli > namespacemanagement content library list`

4 Ejecute el siguiente comando para asociar la biblioteca de contenido al espacio de nombres.

   La operación de actualización no es incremental. Solo las bibliotecas que se especifiquen en la lista se asociarán al espacio de nombres y se eliminarán las bibliotecas que se agregaron anteriormente, a menos que se especifiquen sus identificadores. Por ejemplo, si actualiza `'[{"content_library": "CLA", "writable": "true"}]'` y, a continuación, actualiza `'[{"content_library": "CLB", "writable": "true"}]'`, se eliminará CLA y solo se agregará CLB. Si desea que tanto CLA como CLB se asocien, debe especificar las dos bibliotecas: `'[{"content_library": "CLA", "writable": "true"}, {"content_library": "CLB", "writable": "true"}]'`.

   ```
   dcli > namespaces instances update --namespace namespace_name --content-libraries
   '[{"content_library": "content_library_ID", "writable": "true | false"}]'
   ```

   Utilice los siguientes argumentos:

   - `--namespace namespace_name`: nombre del espacio de nombres.

- `--content_libraries` *`content_library_ID`* `writable: true | false`: identificador de la biblioteca de contenido que se asociará al espacio de nombres y determinará si se puede escribir en la biblioteca o no.

Por ejemplo:

```
dcli > namespaces instances update --namespace lb-edit-ns --content-libraries
'[{"content_library": "cl-b585915ddxxxxxxxx", "writable": "true"}]'
```

5 Para eliminar la biblioteca de contenido del espacio de nombres, repita el comando `namespaces instances update` con el que se elimina la entrada de la biblioteca de contenido de la lista de matrices.

Por ejemplo:

```
dcli > namespaces instances update --namespace lb-edit-ns --content-libraries '[]'
```

Resultados

La biblioteca de contenido agregada estará disponible en la vista del espacio de nombres de desarrollo y operaciones.

El usuario de desarrollo y operaciones puede ejecutar los siguientes comandos para comprobar que la biblioteca de contenido se haya agregado o eliminado.

```
kubectl get cl -n lb-edit-ns
   NAMESPACE    NAME                   VSPHERENAME   TYPE    WRITABLE   STORAGETYPE   AGE
   lb-edit-ns   cl-b585915ddxxxxxxxx   Test-ns-cl    Local   true       Datastore     3m9s
kubectl describe cl cl-b585915ddxxxxxxxx -n lb-edit-ns
kubectl get clitem -n lb-edit-ns
```

Agregar una biblioteca de contenido de máquina virtual a Supervisor mediante la CLI del centro de datos

Además de asignar la biblioteca de contenido en un nivel de espacio de nombres, el administrador de vSphere puede utilizar el comando de la CLI del centro de datos (DCLI, Data Center CLI) para asociar la biblioteca a un clúster de Supervisor. La biblioteca de contenido queda disponible para todos los espacios de nombres del Supervisor.

Puede asociar todo tipo de bibliotecas, incluidas las locales, publicadas y suscritas.

Nota La biblioteca de contenido que se asocie al Supervisor será de solo lectura. Los usuarios de desarrollo y operaciones solo podrán acceder a imágenes de máquina virtual desde esta biblioteca de contenido, pero no podrán publicar imágenes de máquina virtual en ella.

Requisitos previos

Para obtener más información sobre los comandos de la DCLI, consulte CLI de centro de datos de VMware.

Procedimiento

1 Inicie sesión en vCenter Server con la cuenta de usuario raíz.

2 Escriba `dcli +i` para utilizar la DCLI en modo interactivo.

3 Obtenga el nombre del Supervisor y el identificador de la biblioteca de contenido para conectarse al Supervisor.

   a Obtenga el nombre del Supervisor de la lista de clústeres.

   El comando enumera todos los clústeres disponibles en vCenter Server.

   `dcli > namespacemanagement clusters list`

   b Enumere los identificadores de todas las bibliotecas de contenido de cualquier tipo que estén disponibles en vCenter Server.

   `dcli > library list`

   c Compruebe los detalles de la biblioteca específica.

   `dcli > library get --library-id content_library_ID`

4 Asocie una o varias bibliotecas de contenido al Supervisor.

   La operación de actualización no es incremental. Solo las bibliotecas que se especifiquen en la lista se asociarán al espacio de nombres y se eliminarán las bibliotecas que se agregaron anteriormente, a menos que se especifiquen sus identificadores. Por ejemplo, si actualiza `'[{"content_library": "CLA", "writable": "true"}]'` y, a continuación, actualiza `'[{"content_library": "CLB", "writable": "true"}]'`, se eliminará CLA y solo se agregará CLB. Si desea que tanto CLA como CLB se asocien, debe especificar las dos bibliotecas: `'[{"content_library": "CLA", "writable": "true"}, {"content_library": "CLB", "writable": "true"}]'`.

```
dcli > namespacemanagement clusters update --cluster cluster_name --content-libraries
'[{"content_library": content_library_ID_1}, {"content-library": content_library_ID_2}]'
```

   Utilice los siguientes argumentos:

   - `--cluster cluster_name`: identificador del clúster del Supervisor.
   - `--content-libraries content_library_ID`: identificador de una biblioteca de contenido que se asociará al Supervisor. Puede enumerar varios identificadores.

     Por ejemplo:

```
dcli > namespacemanagement clusters update --cluster cluster_name --content-libraries
'[{"content_library": 535d4b3d-xxxx-xxxx-xxxx-xxxxxxxxxxxx}, {"content-library":
b5aa7f68-xxxx-xxxx-xxxx-xxxxxxxxxxxx}]'
```

5 Compruebe que las bibliotecas de contenido estén conectadas al clúster.

```
dcli > namespacemanagement clusters get --cluster cluster_name
```

El resultado debe incluir los identificadores de las bibliotecas de contenido conectadas.

6 Para eliminar la biblioteca de contenido asociada del clúster, repita el comando `namespacemanagement clusters update` con el que se elimina la entrada de la biblioteca de contenido de la lista de matrices de bibliotecas de contenido.

Por ejemplo:

```
dcli > namespacemanagement clusters update --cluster cluster_name --content-libraries '[]'
```

Resultados

Las bibliotecas de contenido recién agregadas pasan a estar disponibles en la vista de clústeres de desarrollo y operaciones. Los cambios que hace el administrador de vSphere en las bibliotecas de contenido se reflejan en la vista de desarrollo y operaciones. El usuario de desarrollo y operaciones puede ejecutar los siguientes comandos para enumerar las bibliotecas de contenido y describir su contenido:

- `kubectl get ccl`: lista de todas las bibliotecas de contenido disponibles en el nivel del clúster. Los resultados son similares a los siguientes.

```
NAME                    VSPHERENAME                         TYPE         STORAGETYPE   AGE
cl-f28af8153fb849bd7    Kubernetes Service Content Library  Subscribed   Datastore     6d5h
cl-knounwp7xxxxxxxxx    Image Registry Content Library      Local        Datastore     6d4h
```

- `kubectl get cclitem`: lista de todos los elementos de las bibliotecas de contenido en el nivel del clúster.
- `kubectl describe ccl NAME`: información detallada de una biblioteca de contenido específica en el nivel del clúster.

Administrar y publicar imágenes de la biblioteca de contenido en vSphere IaaS control plane

Después de que un administrador de vSphere asigna bibliotecas de contenido a un espacio de nombres o un clúster, los usuarios de desarrollo y operaciones pueden acceder a la biblioteca y utilizar sus elementos para implementar máquinas virtuales a partir de imágenes de máquina virtual en la biblioteca. Si se puede escribir en la biblioteca asignada al espacio de nombres, los usuarios de desarrollo y operaciones con permisos de edición también pueden administrar los elementos de la biblioteca y publicar nuevas imágenes de máquina virtual.

Nota No hay restricciones en las imágenes de máquina virtual que puede utilizar. Si desea probar las imágenes OVA listas para utilizar, puede descargarlas de la página Imágenes recomendadas. Tenga en cuenta que estas imágenes son solo para uso en la validación técnica. En el entorno de producción, cree imágenes con las revisiones más recientes y la configuración de seguridad requerida que sigan las directivas de seguridad corporativas.

Requisitos previos

Como usuario de desarrollo y operaciones, asegúrese de seguir estos requisitos:

- Tiene permisos de `Edit` en el espacio de nombres de vSphere.
- El administrador de vSphere asignó una biblioteca de contenido en la que se puede escribir al espacio de nombres. Consulte Agregar una biblioteca de contenido de máquina virtual a Supervisor mediante la CLI del centro de datos .
- La biblioteca de contenido es local o publicada. No se pueden editar las bibliotecas suscritas.

Procedimiento

1 Administre los elementos de biblioteca.

   a Compruebe que las bibliotecas de contenido estén disponibles en el espacio de nombres.

   Nota Si desea administrar elementos de biblioteca en la biblioteca o publicar imágenes de máquina virtual en la biblioteca, asegúrese de que el estado de escritura sea true.

```
kubectl get cl -n <namespace-name>
   NAME                    VSPHERENAME    TYPE    WRITABLE   STORAGETYPE   AGE
   cl-b585915ddxxxxxxxx    Test-ns-cl-1   Local   true       Datastore     3m9s
   cl-535d4b3dnxxxyyyyy    Test-ns-cl-1   Local   false      Datastore     3m9s
```

   b Compruebe el contenido de la biblioteca.

```
kubectl get clitem -n <namespace-name>
 NAME                 VSPHERENAME      CONTENTLIBRAYREF        TYPE    READY    AGE
 clitem-d2wnmq.....   item 1           cl-b585915ddxxxxxxxx    Ovf     True     26c
 clitem-55088d.....   item 2           cl-b585915ddxxxxxxxx    Ovf     True     26c
 clitem-xyzxyz.....   xyzxyz           cl-535d4b3dnxxxyyyyy    Ovf     True     26c
```

c Elimine una imagen de la biblioteca de contenido.

Nota Solo puede eliminar un elemento de la biblioteca en el que se pueda escribir y si tiene permisos de `Edit` o permisos de un nivel superior.

Una vez que se elimina el elemento CLItem, también se elimina el recurso de VMI correspondiente.

```
kubectl delete clitem clitem-55088d.....
 NAME                 VSPHERENAME     CONTENTLIBRAYREF        TYPE   READY   AGE
 clitem-d2wnmq.....   item 1          cl-b585915ddxxxxxxxx    Ovf    True    26c
 clitem-xyzxyz.....   xyzxyz          cl-535d4b3dnxxxyyyyy    Ovf    True    26c
```

d Obtiene los detalles de la imagen.

```
kubectl get vmi -n <namespace-name>
 NAME              PROVIDER-NAME      CONTENT-LIBRARY-NAME    IMAGE-NAME VERSION   OS-
TYPE         FORMAT   AGE
 vmi-d2wnmq.....   clitem-d2wnmq..... cl-b585915ddxxxxxxxx   item 1
ubuntu64guest  ovf      26c
 vmi-55088d.....   clitem-55088d..... cl-b585915ddxxxxxxxx   item 2
otherguest     ovf      26c
```

2 Publique una imagen en la biblioteca de contenido.

a Cree un archivo yaml para implementar una máquina virtual de origen.

Asegúrese de que imageName en la especificación de máquina virtual haga referencia a una de las imágenes de máquina virtual de la biblioteca de contenido.

Por ejemplo, `source-vm.yaml`.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: source-vm
  namespace: test-publish-ns
spec:
  className: best-effort-small
  storageClass: wcpglobal-storage-profile
  imageName: vmi-d2wnmq.....
  powerState: poweredOn
  vmMetadata:
    transport: CloudInit
```

b Obtenga información sobre la máquina virtual implementada y conéctese a la máquina virtual para asegurarse de que se esté ejecutando.

Verá resultados similares al siguiente.

```
kubectl get vm -n <namespace-name>
NAME        POWER-STATE   CLASS              IMAGE           PRIMARY-IP        AGE
source-vm   poweredOn     best-effort-small vmi-d2wnmq..... 192.168.000.00    9m32s
```

c Cree una solicitud de publicación para una nueva imagen de destino.

Por ejemplo, `vmpub.yaml`. En la solicitud, indique el nombre de la máquina virtual de origen y la biblioteca de contenido de destino en la que desea publicar la imagen. Asegúrese de que se pueda escribir en la biblioteca.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachinePublishRequest
metadata:
  name: vmpub-1
  namespace: test-publish-ns
spec:
  source:
    apiVersion: vmoperator.vmware.com/v1alpha2
    kind: VirtualMachine
    name: source-vm # If empty, the name of this VirtualMachinePublishRequest will be 
used as the source VM name ("vmpub-1" in this example).
  target:
    item:
      name: publish-image-1 # If empty, the target item name is <source-vm-name>-image 
by default
    location:
      apiVersion: imageregistry.vmware.com/v1alpha2
      kind: ContentLibrary
      name: cl-b585915ddxxxxxxxx
```

d Describa la solicitud de publicación.

Asegúrese de que la solicitud de publicación tenga el estado `Ready` con `ImageName` establecido.

```
kubectl describe vmpub vmpub-1 -n <namespace-name>
==================
Status:
  imageName: vmi-12980cddd...
  ready: true
==================
```

e Compruebe que la nueva imagen se agregue a la biblioteca de contenido después de que se complete la solicitud de publicación.

```
kubectl get vmi
 NAME               PROVIDER-NAME      CONTENT-LIBRAY-NAME    IMAGE-NAME      VERSION 
OS-TYPE         FORMAT   AGE
 vmi-12980cddd..   clitem-12980cddd.. cl-b585915ddxxxxxxxx   publish-image-1 
ubuntu64guest  ovf      7m12s
 vmi-d2wnmq.....   clitem-d2wnmq..... cl-b585915ddxxxxxxxx   item 1 
ubuntu64guest  ovf      26m
 vmi-55088d.....   clitem-55088d..... cl-b585915ddxxxxxxxx   item 2 
otherguest     ovf      26m
```

Puede utilizar esta nueva imagen para implementar una nueva máquina virtual.

Trabajar con clases de máquinas virtuales en vSphere IaaS control plane

Para poder realizar el autoservicio de máquinas virtuales en vSphere IaaS control plane, los usuarios de desarrollo y operaciones deben tener acceso a las clases de máquinas virtuales. Una clase de máquina virtual es una plantilla que define la CPU, la memoria y las reservas para las máquinas virtuales. La clase de máquina virtual ayuda a establecer barreras para la directiva y el gobierno de las máquinas virtuales, anticipando las necesidades de desarrollo y teniendo en cuenta las restricciones y la disponibilidad de recursos.

vSphere IaaS control plane ofrece varias clases de máquinas virtuales predeterminadas. Un administrador de vSphere puede utilizarlas tal cual está o crear clases de máquinas virtuales personalizadas. Para que las clases estén disponibles para los usuarios de desarrollo y operaciones, el administrador de vSphere las agrega a un espacio de nombres. Las clases de máquinas virtuales asignadas al espacio de nombres pueden ser utilizadas por máquinas virtuales independientes y por las máquinas virtuales que conforman clústeres de Tanzu Kubernetes Grid.

Crear una clase de máquina virtual personalizada mediante vSphere Client

Como administrador vSphere, puede utilizar las clases predeterminadas disponibles. También puede crear clases de máquinas virtuales personalizadas en lugar de las predeterminadas y utilizarlas para la implementación de máquinas virtuales en un espacio de nombres.

Al crear nuevas clases, tenga en cuenta las siguientes consideraciones.

- Las clases de máquinas virtuales que se crean en una instancia de vCenter Server están disponibles para todos los clústeres de vCenter Server y todos los espacios de nombres de estos clústeres.
- Las clases de máquinas virtuales están disponibles para todos los espacios de nombres de vCenter Server. Sin embargo, los ingenieros de desarrollo y operaciones pueden utilizar solo las clases de máquinas virtuales que se asocian con un espacio de nombres en particular.

Nota También puede crear clases de máquina virtual mediante el comando DCLI. Consulte Crear y administrar clases de máquina virtual mediante la CLI del centro de datos.

Requisitos previos

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**
- **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 Desplácese a la página **Servicio de máquina virtual**.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**.

2 En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales** y, a continuación, haga clic en **Crear clase de máquina virtual**.

3 En la página **Nombre**, especifique el nombre de la clase de máquina virtual y haga clic en **Siguiente**.

   El nombre de la clase de máquina virtual identifica la clase de máquina virtual. Introduzca un nombre único conforme con DNS que cumpla estos requisitos:

   - Utilice un nombre único que no sea un duplicado de los nombres de las clases de máquinas virtuales predeterminadas o personalizadas de su entorno.
   - Utilice una cadena alfanumérica con una longitud máxima de 63 caracteres.
   - No utilice caracteres en mayúscula ni espacios.
   - Puede utilizar guiones en cualquier lugar, excepto como primer o último carácter. Por ejemplo, **`vm-class1`**.

   Después de crear la clase de máquina virtual, no puede cambiarle el nombre.

4 En la página **Compatibilidad**, seleccione la compatibilidad del hardware de la clase de máquina virtual y haga clic en **Siguiente**.

   Para obtener más información, consulte Compatibilidad de máquinas virtuales para obtener más información.

   Nota Solo puede establecer la compatibilidad de hardware de una clase de máquina virtual durante su creación y no podrá cambiarla más adelante.

5 En la página **Configuración**, deje los valores predeterminados.

6 En la página **Revisar y Confirmar**, revise los detalles y haga clic en **Finalizar**.

Pasos siguientes

Edite la configuración de la clase de máquina virtual, como el hardware de máquina virtual y las opciones de máquina virtual.

Editar una clase de máquina virtual mediante vSphere Client

Consulte cómo editar una clase de máquina virtual después de su creación. Puede configurar recursos de hardware, como CPU, memoria y dispositivos, así como editar opciones de máquina virtual y parámetros avanzados. También puede editar las clases de máquinas virtuales predeterminadas que ofrece vSphere IaaS control plane.

La edición de una clase de máquina virtual no da como resultado la reconfiguración automática de las máquinas virtuales que se implementaron previamente a partir de esta clase. Por ejemplo, si un usuario de desarrollo y operaciones creó un clúster de Tanzu Kubernetes Grid con una clase de máquina virtual y, posteriormente, usted cambia la definición de esa clase, las máquinas virtuales de Tanzu Kubernetes Grid existentes no se verán afectadas. Las nuevas máquinas virtuales de Tanzu Kubernetes Grid utilizarán la definición de clase modificada.

Precaución Si se escala horizontalmente un clúster de Tanzu Kubernetes Grid después de editar una clase de máquina virtual utilizada por ese clúster, los nuevos nodos del clúster utilizan la definición de clase actualizada, pero los nodos del clúster existentes siguen usando la definición de clase inicial, lo que provoca un error de coincidencia. Tanto los nodos de plano de control como los nodos de trabajo pueden escalarse. Para obtener información sobre el escalado, consulte Escalar un clúster de carga de trabajo en la *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Cuando se elimina una clase de máquina virtual, se la elimina de todos los espacios de nombres asociados. Los usuarios de desarrollo y operaciones ya no pueden usar esa clase de máquina virtual para realizar el autoservicio de las máquinas virtuales. Las máquinas virtuales que ya se crearon con esa clase de máquina virtual no se ven afectadas.

Requisitos previos

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**
- **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 En vSphere Client, muestre las clases de máquinas virtuales disponibles.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Servicios** y haga clic en el panel **Servicio de máquina virtual**.

   c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales**.

   Todas las clases de máquinas virtuales predeterminadas o creadas por el usuario aparecen en **Clases de máquinas virtuales disponibles**.

2 En el panel de la clase de máquina virtual seleccionada, haga clic en **Administrar** y, luego, en **Editar**.

3 En la página **Hardware virtual**, configure los recursos de hardware de la clase de máquina virtual, como la memoria, la CPU y los diferentes dispositivos.

Toda la configuración de hardware de máquina virtual se aplica cuando un usuario de desarrollo y operaciones asigna la clase de máquina virtual a una máquina virtual. Por ejemplo, los valores de configuración de la CPU se convierten en los recursos de CPU dedicados para todas las máquinas virtuales que el usuario de desarrollo y operaciones crea mediante la clase de máquina virtual.

Nota A partir de vSphere 8.0 Update 2b, el asistente que se utiliza para crear y editar clases de máquinas virtuales pasa de establecer recursos de memoria y CPU en porcentajes a valores numéricos en MB, GB, TB y MHz. En todas las clases de máquinas virtuales creadas anteriormente, verá la CPU y la memoria en porcentajes, pero ahora puede editar estos valores en los nuevos formatos numéricos.

Opción Configuración de máquina virtual	Descripción
CPU	Defina los recursos de CPU dedicados a la máquina virtual. Para obtener más información sobre cómo configurar los recursos de CPU, consulte Configuración y limitaciones de la CPU virtual y Configurar recursos de CPU de una máquina virtual.
Memoria	Defina la memoria configurada para una máquina virtual en MB, GB o TB. Para obtener más información sobre los recursos de memoria de máquina virtual, consulte Configurar memoria virtual.
Tarjeta de vídeo	Configure los gráficos 3D para aprovechar Windows AERO, CAD, Google Earth y otras aplicaciones multimedia, de diseño 3D y de modelado. Para obtener más información sobre la configuración de tarjetas de vídeo, consulte Cómo configurar gráficos en 3D.
Dispositivos de seguridad	Proporcione más seguridad a la clase de máquina virtual mediante la configuración de ® Software Guard Extensions (vSGX). Consulte Proteger máquinas virtuales con Intel Software Guard Extensions.

4 En la opción **Hardware virtual**, haga clic en **Agregar nuevo dispositivo** para agregar y configurar dispositivos a la clase de máquina virtual.

Configure diferentes dispositivos para la clase de máquina virtual, como controladores de almacenamiento, adaptadores de red, dispositivos USB y PCI.

Opción Configuración de máquina virtual	Descripción
Disco RDM	Añada una asignación de dispositivos sin formato (RDM, raw device mapping) para almacenar los datos de las máquinas virtuales directamente en un LUN de SAN, en lugar de almacenarlos en un archivo de disco virtual. Consulte Agregar un disco RDM a una máquina virtual.
Dispositivo USB de host	Agregue uno o varios dispositivos USB de acceso directo procedentes de un host ESXi a una máquina virtual si los dispositivos físicos están conectados al host en el que se ejecuta la máquina virtual. Consulte Agregar dispositivos USB de un host ESXi a una máquina virtual.
NVDIMM	Configure un dispositivo NVDIMM virtual en la clase de máquina virtual para que pueda usar la memoria del equipo no volátil o persistente. Consulte Agregar un dispositivo NVDIMM a una máquina virtual.
Unidad de CD/DVD	Configure un dispositivo de CD/DVD en la clase de máquina virtual. Consulte Cómo agregar o modificar una unidad de CD o DVD de máquina virtual.
Controladora NVMe, **Controladora SATA**, **Controladora SCSI**	Configure las controladoras de almacenamiento en la clase de máquina virtual. Consulte Condiciones, limitaciones y compatibilidad de las controladoras de almacenamiento NVMe, SCSI y SATA.
Controladora USB	Agregue una controladora USB a la clase de máquina virtual para admitir el acceso directo de USB desde un host ESXi o desde un recurso informático de cliente. Consulte Agregar una controladora USB a una máquina virtual.
Dispositivo PCI	Configure las máquinas virtuales para que usen la tecnología de GPU virtual (vGPU) NVIDIA GRID si los hosts ESXi del entorno de vSphere IaaS control plane tienen uno o varios dispositivos de gráficos de GPU NVIDIA GRID. También se pueden configurar otros dispositivos PCI en un host ESXi para que estén disponibles para una máquina virtual en modo de acceso directo. Si selecciona esta opción, el valor de reserva de recursos de memoria cambia automáticamente al 100 %. Para obtener más información y los requisitos adicionales, consulte Implementar una máquina virtual con Dispositivos PCI en vSphere IaaS control plane.
Temporizador de Watchdog	Agregue un dispositivo de temporizador de Watchdog virtual (Virtual Watchdog Timer, VWDT) para garantizar la autosuficiencia en relación con el rendimiento del sistema dentro de una máquina virtual. Consulte Cómo agrego un dispositivo temporizador guardián virtual a una máquina virtual.

Opción Configuración de máquina virtual	Descripción
Reloj de precisión	Agregue un dispositivo de reloj de precisión a la máquina virtual. Un reloj de precisión es un dispositivo de reloj virtual que proporciona a una máquina virtual acceso a la hora del sistema del host ESXi principal. Consulte Cómo agregar un dispositivo de reloj de precisión a una máquina virtual.
Puerto serie	Configure una conexión del puerto serie virtual en un puerto serie físico o en un archivo del equipo host. Consulte Cambiar la configuración del puerto serie.
Almacenamiento de instancias	Configure el almacenamiento de instancias en la máquina virtual. Junto con los volúmenes de almacenamiento persistente, una máquina virtual puede utilizar el almacenamiento de instancias. A diferencia de los volúmenes persistentes que existen por separado de la máquina virtual, los volúmenes de almacenamiento de instancias dependen del ciclo de vida de una instancia de máquina virtual. Con la opción **Almacenamiento de instancias**, puede agregar directivas de almacenamiento adecuadas y configurar los volúmenes que se utilizarán con la máquina virtual. Para ver los requisitos adicionales, consulte Implementar una máquina virtual con almacenamiento de instancias en vSphere IaaS control plane.
Adaptador de red	Configure un adaptador de red en la clase de máquina virtual. Cuando el usuario de desarrollo y operaciones implementa una máquina virtual mediante la clase de máquina virtual, puede especificar una red de cargas de trabajo para el adaptador. La red de cargas de trabajo debe configurarse en el espacio de nombres de vSphere en el que se ejecuta la máquina virtual. Para obtener más información sobre los tipos de adaptadores compatibles, consulte Aspectos básicos del adaptador de red.

5 En la página **Opciones de máquina virtual**, puede establecer o cambiar las opciones de máquina virtual para ejecutar scripts de VMware Tools, controlar el acceso de los usuarios a la consola remota, configurar el comportamiento de inicio y más.

   Para obtener más información sobre las opciones de máquina virtual que puede configurar en la clase de máquina virtual, consulte Configurar opciones de máquinas virtuales.

6 En la página **Parámetros avanzados**, puede cambiar o agregar parámetros de configuración de máquina virtual cuando se lo indica un representante del soporte técnico de VMware o si ve documentación de VMware que le indique agregar o cambiar un parámetro para solucionar un problema en el sistema.

   Para obtener más información sobre los parámetros avanzados de la máquina virtual, consulte Configurar parámetros de archivo avanzados de la máquina virtual.

7 Una vez que tenga todo listo para editar la clase de máquina virtual, revise y confirme los cambios y haga clic en **Finalizar**.

Asociar una clase de máquina virtual a un espacio de nombres mediante vSphere Client

Como administrador de vSphere, agregue una clase de máquina virtual predeterminada o personalizada a uno o varios espacios de nombres en un Supervisor. Cuando se agrega una clase de máquina virtual a un espacio de nombres, la clase queda disponible para los usuarios de desarrollo y operaciones, para que puedan iniciar máquinas virtuales de autoservicio en el entorno del espacio de nombres de Kubernetes. Las clases de máquinas virtuales que usted asigna al espacio de nombres también las utilizan las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes Grid.

Puede agregar varias clases de máquinas virtuales a un único espacio de nombres. Las diferentes clases de máquinas virtuales sirven como indicadores de diferentes niveles de servicio. Si publica varias clases de máquinas virtuales, los usuarios de desarrollo y operaciones pueden seleccionar entre todas las clases personalizadas y predeterminadas al crear y administrar máquinas virtuales en el espacio de nombres.

Nota Para poder implementar un clúster de Tanzu Kubernetes Grid en un espacio de nombres recién creado, los ingenieros de desarrollo y operaciones deben tener acceso a las clases de máquinas virtuales. Como administrador de vSphere, debe asociar explícitamente las clases de máquinas virtuales predeterminadas o personalizadas a cualquier nuevo espacio de nombres donde se implemente el clúster de Tanzu Kubernetes Grid.

Requisitos previos

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**
- **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.
   - a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
   - b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue una clase de máquina virtual.
   - a En el panel **Servicio de máquina virtual**, haga clic en **Agregar clase de máquina virtual**.
   - b Seleccione una o varias clases de máquinas virtuales y haga clic en **Aceptar**.

Resultados

Las clases de máquinas virtuales que agregó quedan disponibles en el espacio de nombres para que desarrollo y operaciones realice el autoservicio de las máquinas virtuales. Estas clases también las pueden utilizar las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes Grid.

Administrar clases de máquinas virtuales en un espacio de nombres con vSphere Client

Después de asociar una clase de máquina virtual con un espacio de nombres, puede agregar más clases de máquinas virtuales o eliminar la clase para cancelar su publicación en el espacio de nombres de Kubernetes.

Requisitos previos

- Si desea quitar una clase de máquina virtual de un espacio de nombres, compruebe que Tanzu Kubernetes Grid no la utilice. Su eliminación puede afectar las operaciones de Tanzu Kubernetes Grid.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**
  - **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue o elimine una clase de máquina virtual.

   a En el panel **Servicio de máquina virtual**, haga clic en **Administrar clase de máquina virtual**.

   b Realice una de las siguientes operaciones.

Opción	Descripción
Quitar una clase de máquina virtual	Anule la selección de la clase de máquina virtual y haga clic en **Aceptar**.
Agregar una clase de máquina virtual	Seleccione una o varias clases de máquinas virtuales y haga clic en **Aceptar**.

Crear y administrar clases de máquina virtual mediante la CLI del centro de datos

Además de vSphere Client, puede utilizar los comandos de la CLI del centro de datos (DCLI) para crear y administrar las clases de máquina virtual. Los comandos de la DCLI ofrecen más flexibilidad y acceso a las opciones de configuración de máquina virtual que no están disponibles en vSphere Client.

Requisitos previos

Inicie sesión en vCenter Server con la cuenta de usuario raíz y escriba `dcli +i` para utilizar DCLI en modo interactivo.

Para obtener información sobre los comandos de la DCLI, consulte Descripción de la ejecución de comandos de la DCLI.

Comandos de DCLI disponibles

Comando	Descripción
`namespacemanagement virtualmachineclasses create`	Cree un objeto de clase de máquina virtual.
`namespacemanagement virtualmachineclasses delete`	Elimine el objeto de clase de máquina virtual.
`namespacemanagement virtualmachineclasses get`	Devuelva información sobre una clase de máquina virtual.
`namespacemanagement virtualmachineclasses list`	Devuelva información sobre todas las clases de máquina virtual.
`namespacemanagement virtualmachineclasses update`	Actualice la configuración del objeto de clase de máquina virtual.

Crear una clase de máquina virtual mediante la CLI del centro de datos

Como administrador de vSphere, utilice el comando `com vmware vcenter namespacemanagement virtualmachineclasses create` de la DCLI para crear una clase de máquina virtual. Puede configurar propiedades de máquina virtual como CPU, memoria, reservas de memoria, adaptadores de red, etc.

El comando utiliza los siguientes argumentos.

Argumento	Descripción
-h, --help	Muestra este mensaje de ayuda y sal.
--config-spec CONFIG_SPEC	Una instancia de VirtualMachineConfigSpec asociada a la clase de máquina virtual (entrada json).
--cpu-count CPU_COUNT	Requerido. Número de CPU configuradas para la máquina virtual de esta clase (entero).

Argumento	Descripción
--cpu-reservation CPU_RESERVATION	Porcentaje del total de CPU disponibles reservado para una máquina virtual (entero).
--description DESCRIPTION	Descripción de la clase de máquina virtual (cadena).
--devices-dynamic-direct-path-io-devices DEVICES_DYNAMIC_DIRECT_PATH_IO_DEVICES	Lista de dispositivos de DirectPath I/O dinámicos (entrada json).
--devices-vgpu-devices DEVICES_VGPU_DEVICES	Lista de dispositivos de vGPU (entrada json).
--id ID	Requerido. Identificador de la clase de máquina virtual (cadena).
--instance-storage-policy INSTANCE_STORAGE_POLICY	Directiva de almacenamiento correspondiente al almacenamiento de instancias (cadena).
--instance-storage-volumes INSTANCE_STORAGE_VOLUMES	Lista de volúmenes de almacenamiento de instancias (entrada json).
--memory-mb MEMORY_MB	Requerido. La cantidad de memoria en MB configurada para la máquina virtual de esta clase (entero).
--memory-reservation MEMORY_RESERVATION	El porcentaje de memoria disponible reservado para una máquina virtual de esta clase.

Utilice los siguientes ejemplos para crear clases de máquina virtual con propiedades diferentes.

CPU y memoria

```
com vmware vcenter namespacemanagement virtualmachineclasses create
--id cpu-mem-class --cpu-count 2 --memory-mb 2048 --config-spec
'{"_typeName":"VirtualMachineConfigSpec","numCPUs":2,"memoryMB":2048}'
```

La configuración de `numCPUs` y `memoryMB` en la especificación de configuración es opcional. Si decidió configurarlos, deben tener los mismos valores que los campos de vAPI `--cpu-count` y `--memory-mb` obligatorios.

Reservas de CPU y memoria

Cuando se crea una clase de máquina virtual mediante una especificación de configuración que tiene una reserva de CPU y memoria, el límite o la reserva de memoria se encuentra en MB para `memoryAllocation` y en MHz para `cpuAllocation`.

```
com vmware vcenter namespacemanagement
virtualmachineclasses create --id cpu-res-class-1 --config-
spec '{"_typeName":"VirtualMachineConfigSpec","numCPUs":2,"memoryMB":2048,"cpuAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200},"memoryAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200}}' --cpu-count 2 --
memory-mb 2048
```

Adaptador de red

El siguiente comando crea un adaptador de red de tipo E1000.

```
com vmware vcenter namespacemanagement virtualmachineclasses
create --id class-w-e1000 --cpu-count 2 --memory-
mb 2048 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualE1000","key":-100}}]}'
```

vGPU

En estos ejemplos, el primer comando crea una clase de máquina virtual con una vGPU mediante el campo `--devices-vgpu-devices`. El segundo comando crea una clase de máquina virtual con una vGPU mediante una especificación de configuración.

```
com vmware vcenter namespacemanagement virtualmachineclasses create --id vmclass-1 --devices-
vgpu-devices '[{"profile_name": "mockup-vmiop-8c"}]' --memory-reservation 100 --cpu-count 2 --
memory-mb 4096
```

```
com vmware vcenter namespacemanagement virtualmachineclasses
create --id vmclass-2 --cpu-count 2 --memory-
mb 4096 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-vmiop-8c"}}}]}'
--memory-reservation 100
```

Almacenamiento de instancias

Los siguientes ejemplos crean clases de máquinas virtuales que utilizan el almacenamiento de instancias mediante los campos `--instance-storage-volumes` y `--instance-storage-policy`.

```
com vmware vcenter namespacemanagement virtualmachineclasses create --id vmclass-ist-1
--instance-storage-volumes '[{"size":47}]' --instance-storage-policy "e28d4352-1d1e-431b-
b3f7-528bef5838a0" --cpu-count 2 --memory-mb 4096
```

El campo ID de este ejemplo es un identificador de disco virtual conocido que representa un dispositivo de almacenamiento de instancias en las máquinas virtuales de servicio de máquina virtual.

```
com vmware vcenter namespacemanagement virtualmachineclasses create --id vmclass-ist-2 --cpu-
count 2 --memory-mb 2048 --config-spec
'{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","fileOperation":"create","device":
{"_typeName":"VirtualDisk","key":0,"backing":
{"_typeName":"VirtualDiskFlatVer2BackingInfo","fileName":"","diskMode":"","thinProvisioned":fa
lse},"capacityInKB":0,"capacityInBytes":49283072,"vDiskId":
{"_typeName":"ID","id":"e28d4352-1d1e-431b-b3f7-528bef5838a0"}},"profile":
[{"_typeName":"VirtualMachineDefinedProfileSpec","profileId":"e28d4352-1d1e-431b-
b3f7-528bef5838a0","profileData":
{"_typeName":"VirtualMachineProfileRawData","extensionKey":"com.vmware.vim.sps"}}]}]}'
```

Actualizar una clase de máquina virtual mediante la CLI del centro de datos

Como administrador de vSphere, para modificar una clase de máquina virtual utilice el comando DCLI `com vmware vcenter namespacemanagement virtualmachineclasses update`.

Utilice lo siguiente como ejemplo.

Modificar CPU y memoria

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class cpu-mem-class
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class cpu-mem-class
--cpu-count 4 --memory-mb 4096
```

Modificar reservas de CPU y memoria

Cuando se crea una clase de máquina virtual mediante una especificación de configuración que tiene una reserva de CPU y memoria, el límite o la reserva de memoria se encuentra en MB para `memoryAllocation` y en MHz para `cpuAllocation`.

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class cpu-res-class-1
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class cpu-res-
class-1 --cpu-reservation 100 --memory-reservation 100
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class cpu-res-class-1
```

También puede utilizar las especificaciones de configuración para actualizar las reservas de CPU y memoria. Se sobrescribirá cualquier reserva de CPU o memoria existente. Utilice lo siguiente como ejemplo:

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-
class  cpu-res-class-1 --config-spec '{"_typeName":"VirtualMachineConfigSpec","cpuAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200},"memoryAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200}}'
```

Agregar vGPU

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class class-w-e1000
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class class-w-e1000
--devices-vgpu-devices '[{"profile_name": "mockup-vmiop-8c"}]'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class class-w-e1000
```

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-
class vmclass-1 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-
```

```
vmiop-8c"}}},{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-vmiop"}}}]}'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
```

Eliminar vGPU

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-1 --
devices-vgpu-devices '[]'
 com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
```

Agregar almacenamiento de instancias

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-1
--instance-storage-volumes '[{"size":47}]' --instance-storage-policy "e28d4352-1d1e-431b-
b3f7-528bef5838a0"
 com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
```

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-2
--instance-storage-volumes '[{"size":51},{"size":50}]' --instance-storage-policy
"e28d4352-1d1e-431b-b3f7-528bef5838a0"
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-2
--config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","fileOperation":"create","device":
{"_typeName":"VirtualDisk","key":0,"backing":
{"_typeName":"VirtualDiskFlatVer2BackingInfo","fileName":"","diskMode":"","thinProvisioned":fa
lse},"capacityInKB":0,"capacityInBytes":52428800,"vDiskId":
{"_typeName":"ID","id":"cc737f33-2aa3-4594-aa60-df7d6d4cb984"}},"profile":
[{"_typeName":"VirtualMachineDefinedProfileSpec","profileId":"e28d4352-1d1e-431b-
b3f7-528bef5838a0","profileData":
{"_typeName":"VirtualMachineProfileRawData","extensionKey":"com.vmware.vim.sps"}}]}]}'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
```

Eliminar almacenamiento de instancias

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-1
--instance-storage-volumes '[]' --instance-storage-policy ""
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-1
```

Agregar adaptadores de red

Este comando agrega un almacenamiento de instancias y una NIC e1000 a la clase de máquina virtual.

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-2
--config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","fileOperation":"create","device":
{"_typeName":"VirtualDisk","key":0,"backing":
{"_typeName":"VirtualDiskFlatVer2BackingInfo","fileName":"","diskMode":"","thinProvisioned":fa
lse},"capacityInKB":0,"capacityInBytes":52428800,"vDiskId":
```

```
{"_typeName":"ID","id":"cc737f33-2aa3-4594-aa60-df7d6d4cb984"}},"profile":
[{"_typeName":"VirtualMachineDefinedProfileSpec","profileId":"e28d4352-1d1e-431b-
b3f7-528bef5838a0","profileData":
{"_typeName":"VirtualMachineProfileRawData","extensionKey":"com.vmware.vim.sps"}}]},
{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualE1000","key":-100}}]}'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
```

Especificación de configuración vacía

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class class-w-e1000
--config-spec ''
```

Qué hacer a continuación

Las clases de máquinas virtuales que se crean con DCLI pasan a estar disponibles en vCenter Server. Puede utilizar vSphere Client para asignar estas clases de máquina virtual a un espacio de nombres. Consulte Asociar una clase de máquina virtual a un espacio de nombres mediante vSphere Client.

Implementar una máquina virtual independiente en vSphere IaaS control plane

Como ingeniero de desarrollo y operaciones, utilice el comando `kubectl` para revisar los recursos de máquina virtual disponibles y aprovisionar una máquina virtual de Linux o Windows independiente en un espacio de nombres en un Supervisor. Si la máquina virtual incluye un dispositivo PCI configurado para vGPU, después de crear y arrancar la máquina virtual en el entorno de vSphere IaaS control plane, puede instalar el controlador de gráficos NVIDIA vGPU para habilitar las operaciones de GPU.

Requisitos previos

Para poder implementar una máquina virtual independiente en vSphere IaaS control plane, un ingeniero de desarrollo y operaciones debe tener acceso a recursos específicos de la máquina virtual. Asegúrese de que un administrador de vSphere haya realizado estos pasos para que los recursos de máquina virtual estén disponibles:

- Cree un espacio de nombres y asígnele directivas de almacenamiento. Consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.

- Cree una biblioteca de contenido y asóciela con el espacio de nombres. Consulte Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere IaaS control plane.
  - Si una biblioteca de contenido está protegida por una directiva de seguridad, todos los elementos de la biblioteca deben ser compatibles. Si la biblioteca protegida incluye una combinación de elementos conformes y no conformes, el comando `kubectl get virtualmachineimages` no puede presentar imágenes de máquina virtual a los ingenieros de desarrollo y operaciones.
  - Si tiene pensado implementar máquinas virtuales con dispositivos vGPU, debe poder acceder a las imágenes con el modo de arranque establecido en EFI, como CentOS.
- Asocie clases de máquina virtual predeterminadas o personalizadas con un espacio de nombres. Consulte Trabajar con clases de máquinas virtuales en vSphere IaaS control plane.

Si tiene pensado utilizar vGPU de NVIDIA u otros dispositivos PCI para las máquinas virtuales, debe cumplir con requisitos adicionales. Para obtener información, consulte Implementar una máquina virtual con Dispositivos PCI en vSphere IaaS control plane.

Para obtener información sobre el operador de máquina virtual y los campos compatibles, consulte Conceptos del servicio de máquina virtual y https://vm-operator.readthedocs.io/en/stable/ref/api/v1alpha2/.

Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere IaaS control plane

Como ingeniero de desarrollo y operaciones, compruebe que puede acceder a los recursos de máquinas virtuales en el espacio de nombres y ver las clases y las plantillas de máquina virtual disponibles en su entorno. También puede enumerar las clases de almacenamiento y otros elementos que podría necesitar para realizar el autoservicio de una máquina virtual.

Esta tarea abarca los comandos que se utilizan para acceder a los recursos disponibles para la implementación de una máquina virtual independiente. Para obtener información sobre los recursos necesarios para implementar Tanzu Kubernetes Grid clústeres y máquinas virtuales que conforman los clústeres, consulte Clases de máquinas virtuales para clústeres de TKG en la documentación de *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Procedimiento

1 Acceda al espacio de nombres en el entorno de Kubernetes.

  Consulte Obtener y utilizar el contexto del Supervisor en vSphere IaaS control plane.

2 Para ver las clases de máquina virtual disponibles en el espacio de nombres, ejecute el siguiente comando.

```
kubectl get virtualmachineclass
```

Es posible que se muestre el siguiente resultado.

Nota Debido a que el tipo de clase de máquina virtual de mejor esfuerzo permite que los recursos se sobreasignen, puede quedarse sin recursos si ha establecido límites en el espacio de nombres en el que está aprovisionando las máquinas virtuales. Por este motivo, utilice el tipo de clase de máquina virtual garantizada en el entorno de producción.

```
NAME                        VIRTUALMACHINECLASS        AGE

best-effort-large           best-effort-large          44m
best-effort-medium          best-effort-medium         44m
best-effort-small           best-effort-small          44m
best-effort-xsmall          best-effort-xsmall         44m
custom                      custom                     44m
```

3 Para ver los detalles de una clase de máquina virtual específica, ejecute los siguientes comandos.

- `kubectl describe virtualmachineclasses` *name_vm_class*

  Si una clase de máquina virtual incluye un dispositivo vGPU, puede ver su perfil en `spec: hardware: devices: vgpuDevices`.

  ```
  ......
  spec:
    hardware:
      cpus: 4
      devices:
        vgpuDevices:
        - profileName: grid_v100-q4
  ......
  ```

- `kubectl get virtualmachineclasses -o wide`

  Si la clase de máquina virtual incluye una vGPU o un directo de acceso directo, el resultado lo muestra en la columna `VGPUDevicesProfileNames` o `PassthroughDeviceIDs`.

4 Ver las imágenes de máquina virtual.

`kubectl get virtualmachineimages`

El resultado que ve es similar al siguiente. El nombre de la imagen, como `vmi-xxxxxxxxxxxxx`, es generado automáticamente por el sistema.

```
NAME                                              VERSION  OSTYPE               FORMAT
IMAGESUPPORTED  AGE
vmi-xxxxxxxxxxxxx                                          centos8_64Guest      ovf
true            4d3h
```

5 Para describir una imagen específica, utilice el siguiente comando.

```
kubectl describe virtualmachineimage vmi-xxxxxxxxxxxxx
```

Las máquinas virtuales con dispositivos de vGPU requieren imágenes que tengan el modo de arranque establecido en EFI, como CentOS. Asegúrese de tener acceso a estas imágenes.

6 Compruebe si puede acceder a las clases de almacenamiento.

```
kubectl get resourcequotas
```

Para obtener más información, consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere.

```
NAME                            AGE
REQUEST
     LIMIT
my-ns-ubuntu-storagequota   24h   wcpglobal-storage-profile.storageclass.storage.k8s.io/
requests.storage: 0/9223372036854775807
```

Implementar una máquina virtual en vSphere IaaS control plane

Como ingeniero de desarrollo y operaciones, aprovisione una máquina virtual y su SO invitado de forma declarativa al escribir especificaciones de implementación de máquina virtual en un archivo YAML de Kubernetes.

Requisitos previos

Si utiliza vGPU de NVIDIA u otros dispositivos PCI para sus máquinas virtuales, consulte Implementar una máquina virtual con Dispositivos PCI en vSphere IaaS control plane.

Procedimiento

1 Prepare el archivo YAML de la máquina virtual.

En el archivo, especifique los siguientes parámetros:

Opción	Descripción
apiVersion	Especifica la versión de la API del servicio de máquina virtual. Por ejemplo, **`vmoperator.vmware.com/v1alpha2`**.
kind	Especifica el tipo de recurso de Kubernetes que se debe crear. El único valor disponible es **`VirtualMachine`**.
spec.imageName	Especifica el nombre del recurso de imagen de máquina virtual en el clúster de Kubernetes.
spec.storageClass	Especifica la clase de almacenamiento que se utilizará para el almacenamiento de los volúmenes persistentes.
spec.className	Especifica el nombre de la clase de máquina virtual que describe la configuración de hardware virtual que se utilizará.

Opción	Descripción
spec.networkInterfaces	Especifica la configuración relacionada con la red para la máquina virtual. ■ `networkType`. Los valores para esta clave pueden ser **`nsx-t`** o **`vsphere-distributed`**. ■ `networkName`. Si es necesario, especifique el nombre o deje el nombre predeterminado.
spec.vmMetadata	Incluye metadatos adicionales que se transferirán a la máquina virtual. Puede utilizar esta clave para personalizar la imagen del SO invitado y establecer estos elementos como el `hostname` de la máquina virtual y `user-data`, incluidas las contraseñas, las claves SSH, etc. Para obtener más información, incluidos detalles sobre cómo arrancar y personalizar las máquinas virtuales de Windows mediante la herramienta de preparación del sistema de Microsoft (Sysprep), consulte Personalizar un invitado.
topology.kubernetes.io/zone	Controla la colocación de máquinas virtuales en un Supervisor de tres zonas. Por ejemplo, `topology.kubernetes.io/zone: zone-a02`.

El siguiente ejemplo de archivo YAML de máquina virtual `my-vm` utiliza CloudInit como método de arranque. El ejemplo muestra un recurso de VirtualMachine que especifica los datos de usuario en un recurso secreto `my-vm-bootstrap-data`. El secreto se utilizará para arrancar y personalizar el sistema operativo invitado.

Los datos del secreto incluyen cloud-config de CloudInit. Para obtener más información sobre el formato cloud-config, consulte los ejemplos de configuración de nube en la documentación oficial.

Para ver ejemplos con Sysprep como método de arranque, consulte Sysprep.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name:      my-vm
  namespace: my-namespace
spec:
  className:    small
  imageName:    vmi-xxxxxxxxxxxxx
  storageClass: iscsi
  vmMetadata:
    transport: CloudInit
    secretName: my-vm-bootstrap-data
```

```
apiVersion: v1
kind: Secret
metadata:
  name:      my-vm-bootstrap-data
  namespace: my-namespace
stringData:
  user-data: |
    #cloud-config
    users:
    - default
```

```
    - name: xyz..
      primary_group: xyz..
      groups: users
      ssh_authorized_keys:
      - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSL7uWGj...
    runcmd:
    - "ls /"
    - [ "ls", "-a", "-l", "/" ]
    write_files:
    - path: /etc/my-plaintext
      permissions: '0644'
      owner: root:root
      content: |
        Hello, world.
```

Utilice el siguiente ejemplo si va a implementar una máquina virtual en un entorno con zonas.

Para obtener los valores para *ZONE_NAME*, ejecute el comando `kubectl get vspherezones`.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: <vm-name>
  namespace: <vm-ns>
  labels:
    topology.kubernetes.io/zone: ZONE_NAME
...
```

2 Implemente la máquina virtual.

```
kubectl apply -f my-vm.yaml
```

3 Compruebe que se haya creado la máquina virtual.

```
kubectl get vm
NAME              AGE
my-vm             28s
```

4 Compruebe los detalles de la máquina virtual y su estado.

```
kubectl describe virtualmachine my-vm
```

Los resultados son similares al siguiente. De los resultados también puede obtener la dirección IP de la máquina virtual, que aparece en el campo `Vm Ip`.

```
Name:         my-vm
Namespace:    my-namespace
API Version:  vmoperator.vmware.com/v1alpha2
Kind:         VirtualMachine
Metadata:
  Creation Timestamp:  2021-03-23T19:07:36Z
  Finalizers:
```

```
      virtualmachine.vmoperator.vmware.com
    Generation:  1
    Managed Fields:
   ...
   ...
  Status:
    Bios UUID:              4218ec42-aeb3-9491-fe22-19b6f954ce38
    Change Block Tracking:  false
    Conditions:
      Last Transition Time:  2021-03-23T19:08:59Z
      Status:                True
      Type:                  VirtualMachinePrereqReady
    Host:                    10.185.240.10
    Instance UUID:           50180b3a-86ee-870a-c3da-90ddbaffc950
    Phase:                   Created
    Power State:             poweredOn
    Unique ID:               vm-73
    Vm Ip:                   10.161.75.162
  Events:                    <none>
  ...
```

5 Compruebe que se pueda acceder a la IP de la máquina virtual.

```
ping 10.161.75.162
PING 10.161.75.162 (10.161.75.162): 56 data bytes
64 bytes from 10.161.75.162: icmp_seq=0 ttl=59 time=43.528 ms
64 bytes from 10.161.75.162: icmp_seq=1 ttl=59 time=53.885 ms
64 bytes from 10.161.75.162: icmp_seq=2 ttl=59 time=31.581 ms
```

Resultados

Una máquina virtual creada a través del servicio de máquina virtual solo puede administrarla desarrollo y operaciones desde el espacio de nombres de Kubernetes. Su ciclo de vida no puede administrarse desde vSphere Client, pero los administradores de vSphere pueden supervisar la máquina virtual y sus recursos. Para obtener más información, consulte Supervisar máquinas virtuales disponibles en vSphere IaaS control plane.

Pasos siguientes

Para obtener más información, consulte el blog Introducción al aprovisionamiento de máquinas virtuales.

Implementar una máquina virtual con vGPU y otros dispositivos PCI en vSphere IaaS control plane

Si los hosts ESXi de su entorno de vSphere IaaS control plane tienen uno o varios dispositivos de gráficos de GPU NVIDIA GRID, es posible configurar las máquinas virtuales para que usen esta tecnología de GPU virtual (vGPU) NVIDIA GRID. También se pueden configurar otros dispositivos PCI en un host ESXi para que estén disponibles para una máquina virtual en modo de acceso directo.

Implementar una máquina virtual con vGPU en vSphere IaaS control plane

Los dispositivos de gráficos de GPU NVIDIA GRID están diseñados para optimizar operaciones gráficas complejas y permitir que estas se ejecuten con un alto rendimiento sin sobrecargar la CPU. La unidad de vGPU NVIDIA GRID brinda un rendimiento de gráficos sin igual, economía y escalabilidad, ya que permite compartir una sola GPU física entre varias máquinas virtuales como si fueran dispositivos de acceso directo habilitados para vGPU distintos.

Consideraciones

Las siguientes consideraciones se aplican cuando se utiliza NVIDIA vGPU:

- El Supervisor de tres zonas no admite máquinas virtuales con vGPU.
- Las máquinas virtuales con dispositivos vGPU administradas por el servicio de máquina virtual se apagan automáticamente cuando un host ESXi entra en modo de mantenimiento. Esto puede afectar temporalmente a las cargas de trabajo que se ejecutan en las máquinas virtuales. Las máquinas virtuales se encienden automáticamente después de que el host sale del modo de mantenimiento.
- DRS distribuye las máquinas virtuales de vGPU de manera integral entre los hosts del clúster. Para obtener más información, consulte Colocación de DRS de máquinas virtuales de vGPU en la guía de *Administrar recursos de vSphere*.

Requisitos

Para configurar la vGPU de NVIDIA, siga estos requisitos:

- Compruebe que ESXi sea compatible según la Guía de compatibilidad de VMware y póngase en contacto con el proveedor para comprobar que el host cumpla los requisitos de alimentación y configuración.
- Configure los ajustes de los gráficos de hosts ESXi con al menos un dispositivo en modo **Compartidos directos**. Consulte Configurar gráficos de host en la documentación de *Administrar recursos de vSphere*.
- La biblioteca de contenido que se utiliza para las máquinas virtuales con dispositivos vGPU debe incluir imágenes con el modo de arranque establecido en EFI, como CentOS.
- Instale el software NVIDIA vGPU. NVIDIA proporciona un paquete de software vGPU que incluye los siguientes componentes.

  Para obtener más información, consulte la documentación correspondiente del software NVIDIA Virtual GPU.

  - vGPU Manager que un administrador de vSphere instala en el host ESXi. Consulte el artículo 2033434 de la base de conocimientos de VMware.

- Controlador de máquina virtual invitado que un ingeniero de desarrollo y operaciones instala en la máquina virtual después de implementar y arrancar la máquina virtual. Consulte Instalar el controlador invitado de NVIDIA en una máquina virtual en vSphere IaaS control plane.

Agregar un dispositivo vGPU a una clase de máquina virtual mediante vSphere Client

Cree o edite una clase de máquina virtual existente para agregar una GPU virtual (vGPU) NVIDIA GRID.

Requisitos previos

Privilegios necesarios:

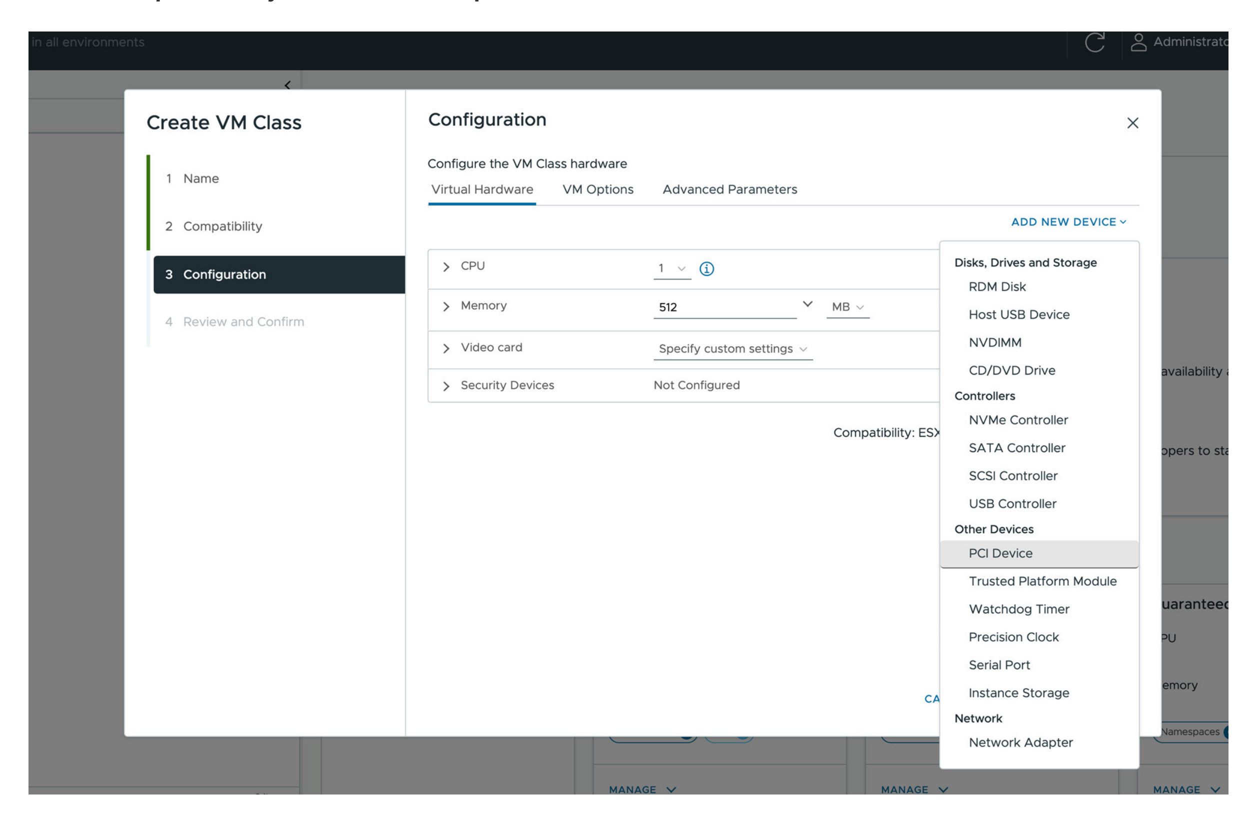
- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**
- **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 Cree o edite una clase de máquina virtual existente.

Opción	Acción
Crear una nueva clase de máquina virtual	a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**. b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**. c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales** y, a continuación, haga clic en **Crear clase de máquina virtual**. d Siga las indicaciones.
Edite una clase de máquina virtual.	a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**. b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**. c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales**. d En el panel de la clase de máquina virtual seleccionada, haga clic en **Administrar** y, luego, en **Editar**. e Siga las indicaciones.

2 En la página **Configuración**, haga clic en la pestaña **Hardware virtual**, haga clic en **Agregar nuevo dispositivo** y seleccione **Dispositivo PCI**.

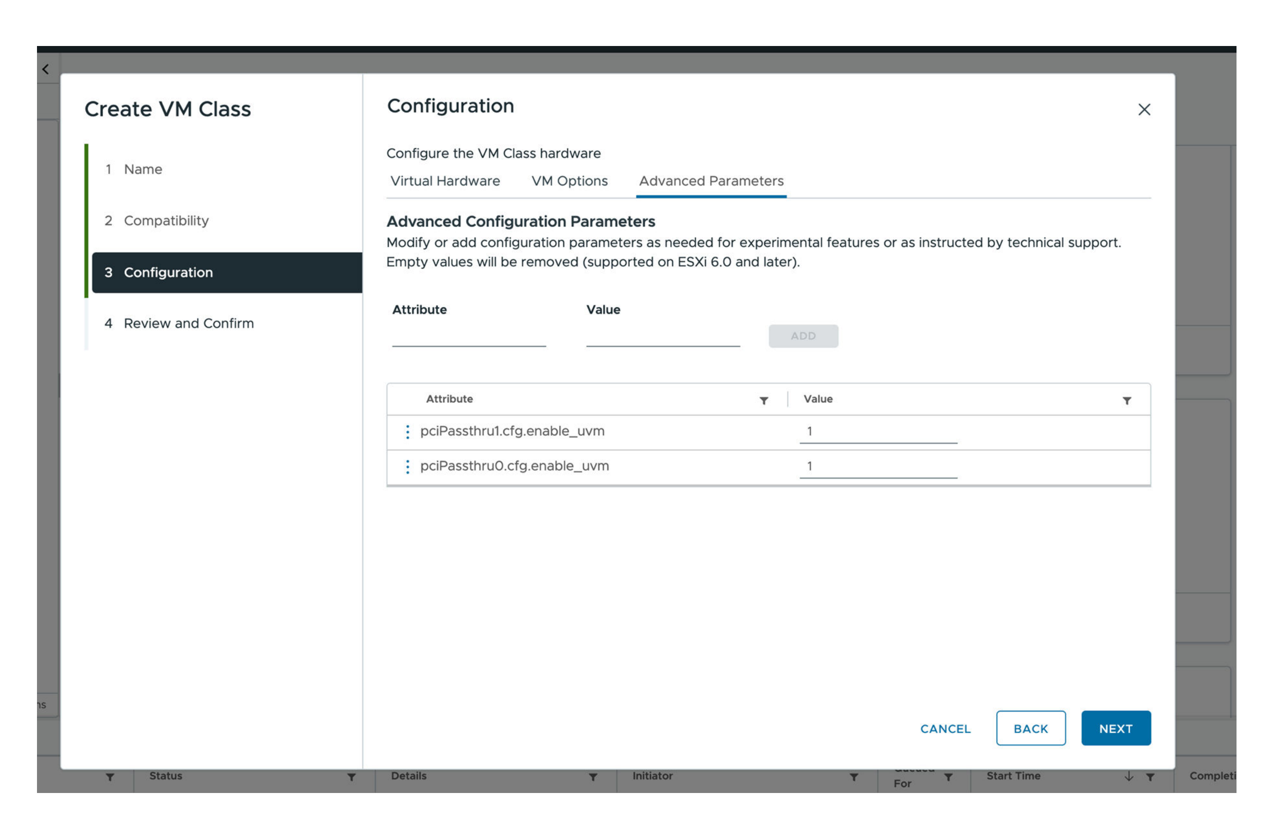


3 En la lista de dispositivos disponibles de la página **Selección de dispositivo**, seleccione NVIDIA GRID vGPU y haga clic en **Seleccionar**.

El dispositivo aparece en la página Hardware virtual.

4 Haga clic en la pestaña **Parámetros avanzados** y establezca los parámetros con los siguientes atributos y valores.

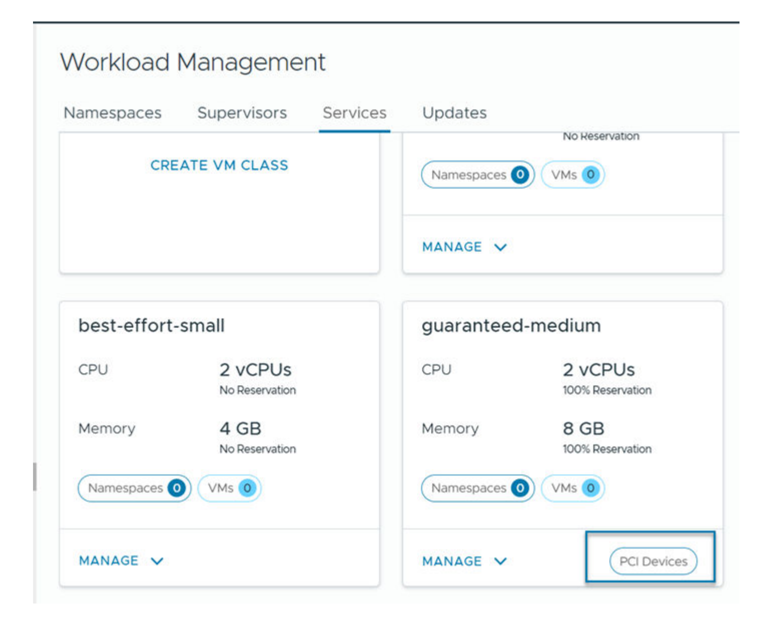
Opción	Descripción
Parámetro	Valor
pciPassthru0.cfg.enable_uvm	1
pciPassthru1.cfg.enable_uvm	1



5 Revise su configuración y haga clic en **Finalizar**.

Resultados

Una etiqueta **Dispositivos PCI** en el panel de clase de máquina virtual indica que la clase de máquina virtual está habilitada para la vGPU.



Agregar un dispositivo vGPU a una clase de máquina virtual mediante la CLI del centro de datos

Además de vSphere Client, puede utilizar el comando de la CLI del centro de datos (DCLI) para agregar varias vGPU y configuraciones avanzadas.

Para obtener más información sobre los comandos de la DCLI, consulte Crear y administrar clases de máquina virtual mediante la CLI del centro de datos.

Procedimiento

1 Inicie sesión en vCenter Server con la cuenta de usuario raíz y escriba `dcli +i` para utilizar la DCLI en modo interactivo.

2 Ejecute el siguiente comando para crear una de clase de máquina virtual.

   En el siguiente ejemplo, la clase de máquina virtual *my-class* incluye dos CPU, 2048 de memoria y una instancia de VirtualMachineConfigSpec con dos perfiles de vGPU de muestra, `mockup-vmiop-8c` y `mockup-vmiop`. Los campos extraConfig `pciPassthru0.cfg.enable_uvm` y `pciPassthru1.cfg.enable_uvm` se establecen en 1.

```
dcli +i +show-unreleased com vmware vcenter namespacemanagement
virtualmachineclasses create --id my-class --cpu-count 2 --memory-
mb 2048 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-
vmiop-8c"}}},{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-
vmiop"}}}],"extraConfig":
[{"_typeName":"OptionValue","key":"pciPassthru0.cfg.enable_uvm","value":
{"_typeName":"string","_value":"1"}},
{"_typeName":"OptionValue","key":"pciPassthru1.cfg.enable_uvm","value":
{"_typeName":"string","_value":"1"}}]}'
```

Instalar el controlador invitado de NVIDIA en una máquina virtual en vSphere IaaS control plane

Si la máquina virtual incluye un dispositivo PCI configurado para vGPU, después de crear y arrancar la máquina virtual en el entorno de vSphere IaaS control plane, instale el controlador de gráficos NVIDIA vGPU para habilitar completamente las operaciones de GPU.

Requisitos previos

- Implemente la máquina virtual con vGPU. Asegúrese de que el archivo YAML de la máquina virtual haga referencia a la clase de máquina virtual con la definición de vGPU. Consulte Implementar una máquina virtual en vSphere IaaS control plane.

- Compruebe que descargó el paquete de software de vGPU del sitio de descargas de NVIDIA, descomprimió el paquete y tiene listo el componente de la unidad de invitado. Para obtener información, consulte la documentación correspondiente del software de GPU virtual de NVIDIA.

  Nota La versión del componente del controlador debe corresponder a la versión de vGPU Manager que un administrador de vSphere instaló en el host ESXi.

Procedimiento

1 Copie el paquete de controladores Linux del software de NVIDIA vGPU, por ejemplo, `NVIDIA-Linux-x86_64-` *versión* `-grid.run`, en la máquina virtual invitada.

2 Antes de intentar ejecutar el instalador del controlador, finalice todas las aplicaciones.

3 Inicie el instalador del controlador NVIDIA vGPU.

```
sudo ./NVIDIA-Linux-x86_64-version-grid.run
```

4 Acepte el acuerdo de licencia de software de NVIDIA y seleccione **Sí** para actualizar automáticamente los ajustes de configuración de X.

5 Compruebe que se haya instalado el controlador.

Por ejemplo:

```
~$ nvidia-smi
Wed May 19 22:15:04 2021
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 460.63       Driver Version: 460.63       CUDA Version: 11.2     |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  GRID V100-4Q        On   | 00000000:02:00.0 Off |                  N/A|
| N/AN/AP0    N/A/  N/A|    304MiB /  4096MiB |      0%      Default |
|                               |                      |                  N/A|
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Implementar una máquina virtual con Dispositivos PCI en vSphere IaaS control plane

Además de una vGPU, se pueden configurar otros dispositivos PCI en un host ESXi para que estén disponibles para una máquina virtual en modo de acceso directo.

vSphere IaaS control plane admite dispositivos de DirectPath I/O dinámico. Mediante la instancia dinámica de DirectPath I/O, la máquina virtual puede acceder directamente a los dispositivos PCI y PCIe físicos conectados a un host. Puede usar la instancia dinámica de DirectPath I/O para asignar varios dispositivos de acceso directo a PCI a una máquina virtual. Cada dispositivo de acceso directo se puede especificar mediante su proveedor de PCI e identificador de dispositivo.

Nota Al configurar una instancia dinámica de DirectPath I/O para dispositivos PCI de acceso directo, conecte los dispositivos PCI al host y márquelos como disponibles para el acceso directo. Consulte Habilitar el acceso directo para un dispositivo de red en un host en la documentación de *Redes de vSphere*.

Implementar una máquina virtual con almacenamiento de instancias en vSphere IaaS control plane

Junto con los volúmenes de almacenamiento persistente, una máquina virtual puede utilizar el almacenamiento de instancias. A diferencia de los volúmenes persistentes que existen por separado de la máquina virtual, los volúmenes de almacenamiento de instancias dependen del ciclo de vida de una instancia de máquina virtual. Por lo general, este almacenamiento se encuentra en dispositivos de alta velocidad, como NVMe, que son locales para el host ESXi.

Ciclo de vida de almacenamiento de instancias

En el proceso de creación de máquinas virtuales, el sistema crea volúmenes de almacenamiento de instancias y los asocia a la máquina virtual. Los datos que están en el volumen de almacenamiento de instancias solo se conservan durante la vida útil de su instancia de máquina virtual asociada. El volumen se elimina cuando lo hace la máquina virtual.

Las máquinas virtuales con almacenamiento de instancias admiten el modo de mantenimiento del host ESXi. La máquina virtual se apaga cuando el host ESXi entra en modo de mantenimiento y se enciende una vez que el host sale del modo de mantenimiento.

Consideraciones sobre la máquina virtual de almacenamiento de instancias

Tenga en cuenta los siguientes elementos cuando utilice máquinas virtuales con almacenamiento de instancias:

- Supervisor con una pila de redes de VDS no admite el almacenamiento de instancias.
- Supervisor de tres zonas no admite el almacenamiento de instancias.

- Aparece una advertencia si un administrador de vSphere aplica una clase de máquina virtual con almacenamiento de instancias a un espacio de nombres que omite una directiva de almacenamiento adecuada que se requiere para el almacenamiento de instancias.
- Las máquinas virtuales con volúmenes de instancias no se pueden migrar a otros hosts ESXi.
- No es posible editar los volúmenes de almacenamiento de instancias cuando los volúmenes ya se están usando.
- Si el administrador de vSphere elimina la directiva de almacenamiento de instancias del espacio de nombres después de crear la máquina virtual, la máquina virtual continúa ejecutándose.
- Como ingeniero de desarrollo y operaciones, no puede eliminar ni actualizar recursos de almacenamiento de instancias. No es posible desasociar el volumen de almacenamiento de instancias de una instancia de máquina virtual y asociarlo a otra instancia.

Flujo de trabajo para aprovisionar y supervisar una máquina virtual de almacenamiento de instancias

Paso	Realizado por	Descripción
1	Administrador de vSphere	Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere IaaS control plane
2	Administrador de vSphere	Cree un almacén de datos de vSAN Direct.
3	Administrador de vSphere	Cree una directiva de almacenamiento compatible con vSAN Direct y asígnela al espacio de nombres.
4	Administrador de vSphere	Cree una clase de máquina virtual de almacenamiento de instancias y asígnela al espacio de nombres.
5	Ingeniero de desarrollo y operaciones	Aprovisione una máquina virtual con almacenamiento de instancias en el espacio de nombres.
6	Administrador de vSphere	Supervisar máquinas virtuales disponibles en vSphere IaaS control plane

Crear un almacén de datos de vSAN Direct

Como administrador de vSphere, configure un almacén de datos de vSAN Direct para utilizarlo con funcionalidades como la plataforma de persistencia de datos de vSAN o el almacenamiento de instancias de máquina virtual. Para crear el almacén de datos, use dispositivos de almacenamiento sin reclamar que estén en el host ESXi.

Puede crear el almacén de datos de vSAN Direct cuando habilite vSAN para el Supervisor. La siguiente tarea muestra cómo se reclaman dispositivos de almacenamiento local como vSAN Direct cuando vSAN ya está habilitado en el clúster.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

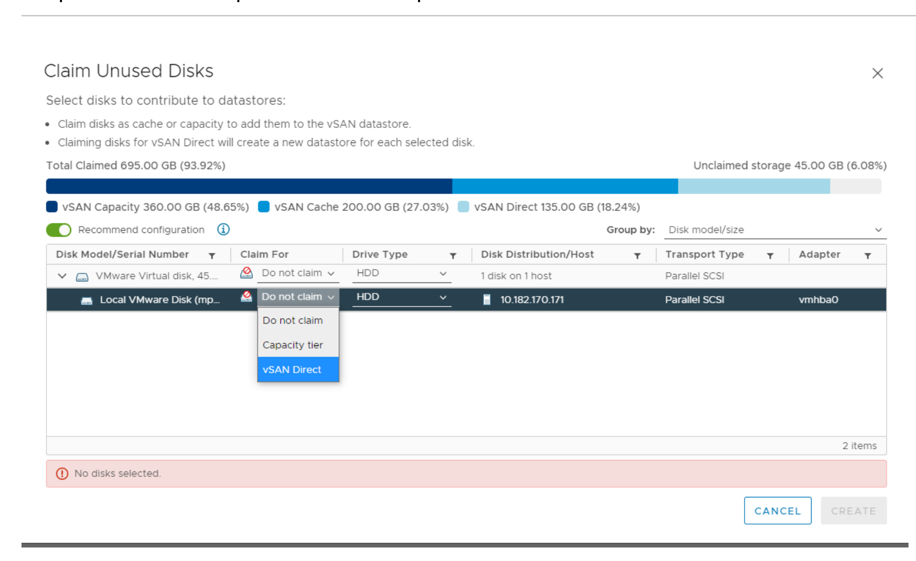
3 En vSAN, haga clic en **Administración de discos**.

4 Haga clic en **Reclamar discos sin utilizar**.

5 En el cuadro de diálogo **Reclamar discos sin utilizar**, haga clic en la pestaña **vSAN Direct**.

6 Seleccione un dispositivo para reclamar y seleccione una casilla de verificación en la columna **Reclamar para vSAN Direct** .

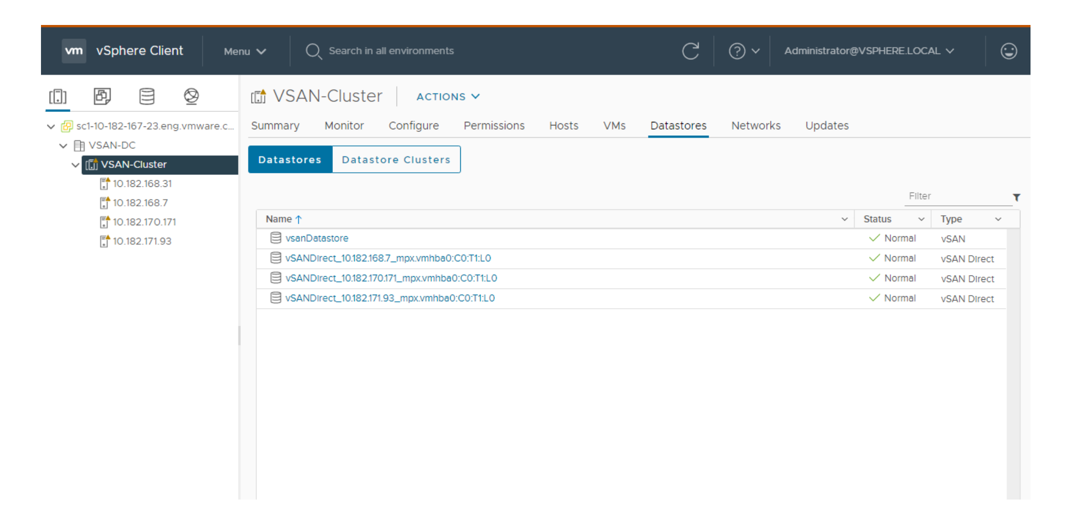
Nota Si reclamó los dispositivos para un almacén de datos de vSAN normal, estos dispositivos no aparecen en la pestaña **vSAN Direct** .



7 Haga clic en **Crear**.

En cada dispositivo que reclame, vSAN Direct crea un almacén de datos nuevo.

8 Haga clic en la pestaña **Almacenes de datos** para mostrar todos los almacenes de datos de vSAN Direct en el clúster.



Pasos siguientes

Puede utilizar vSAN Direct con almacenamiento externo. Para obtener más información, consulte Usar el almacenamiento externo con vSAN Direct en la documentación de *Mantenimiento del plano de control de IaaS de vSphere*.

Crear directiva de almacenamiento de vSAN Direct

Si utiliza vSAN Direct, cree una directiva de almacenamiento que se utilizará con un espacio de nombres de Supervisor. En el espacio de nombres que se asocia con esta directiva de almacenamiento, se pueden ejecutar cargas de trabajo compatibles con vSAN Direct, por ejemplo, servicios con estado o máquinas virtuales de almacenamiento de instancia.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a En el menú **Inicio**, haga clic en **Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva**, en **Reglas específicas de almacenes de datos**, habilite las reglas para la colocación del almacenamiento de vSAN Direct.

4 En la página **Reglas de vSAN Direct**, especifique vSAN Direct como un tipo de colocación de almacenamiento.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos de vSAN Direct que coinciden con esta directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Crear una clase de máquina virtual con almacenamiento de instancias

En la clase de máquina virtual, se hace referencia a la directiva de almacenamiento de vSAN Direct y se establece el tamaño de los volúmenes que se utilizarán para el almacenamiento de instancias. Después de crear la clase de máquina virtual, asígnela al espacio de nombres que planea utilizar para la máquina virtual de almacenamiento de instancias.

Requisitos previos

- Cree una directiva de almacenamiento compatible con el almacén de datos de vSAN Direct.
- Agregue la directiva de almacenamiento de vSAN Direct al espacio de nombres que utiliza para la máquina virtual de almacenamiento de instancias. Consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**
  - **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

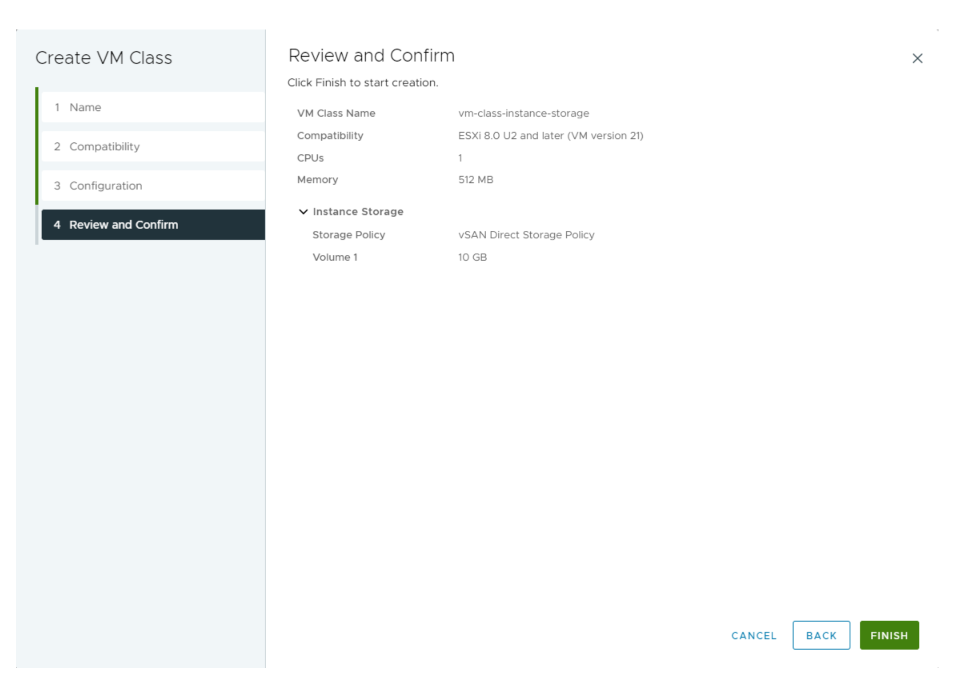
1 Agregue almacenamiento de instancias cuando cree o edite una clase de máquina virtual.

Opción	Acción
Crear una clase de máquina virtual	a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**. b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en la tarjeta **Servicio de máquina virtual**. c En la página **Servicio de máquina virtual**, haga clic en **Crear clase de máquina virtual**. d Configure la clase de máquina virtual según sea necesario; consulte Editar una clase de máquina virtual mediante vSphere Client para ver las opciones disponibles. e Para agregar un almacenamiento de instancias, en la página **Configuración**, seleccione **Hardware virtual** y, a continuación, seleccione **Agregar nuevo dispositivo > Almacenamiento de instancias**. La opción **Almacenamiento de instancias** aparece en Hardware virtual.
Editar una clase de máquina virtual existente	a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**. b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**. c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales**. d En la tarjeta de la clase de máquina virtual seleccionada, haga clic en **Administrar** y, luego, en **Editar**. e Para agregar un almacenamiento de instancias, seleccione **Hardware virtual** y, a continuación, seleccione **Agregar nuevo dispositivo > Almacenamiento de instancias**. La opción **Almacenamiento de instancias** aparece en Hardware virtual.

2 Expanda la opción **Almacenamiento de instancias** para editar la configuración de almacenamiento de instancias.

Opción	Acción
Directiva de almacenamiento	Seleccione la directiva de almacenamiento de vSAN Direct.
Volumen	Especifique el tamaño del volumen. Puede agregar varios volúmenes de almacenamiento.

3 En la página **Revisar y Confirmar**, revise los detalles y haga clic en **Finalizar**.



4 Asigne la clase de máquina virtual que creó al espacio de nombres que utilice para la máquina virtual de almacenamiento de instancias.

Consulte Asociar una clase de máquina virtual a un espacio de nombres mediante vSphere Client.

Implementar una máquina virtual con almacenamiento de instancias

Como ingeniero de desarrollo y operaciones, compruebe que puede acceder a los recursos de máquina virtual necesarios para crear una máquina virtual de almacenamiento de instancias. Utilice los recursos para implementar la máquina virtual.

Cuando implemente la máquina virtual de almacenamiento de instancias, siga los pasos generales de implementación de la máquina virtual. Consulte Implementar una máquina virtual independiente en vSphere IaaS control plane. Este procedimiento abarca elementos específicos adicionales que se aplican a la máquina virtual de almacenamiento de instancias.

Procedimiento

- Compruebe los siguientes elementos específicos de la máquina virtual de almacenamiento de instancias:
  - El espacio de nombres incluye la clase de almacenamiento compatible con el almacén de datos de vSAN Direct.
  - La clase de máquina virtual de almacenamiento de instancias hace referencia a esta clase de almacenamiento.

    Al revisar los detalles de la clase de máquina virtual de almacenamiento de instancias, asegúrese de que incluya la sección `instanceStorage`.

    `kubectl describe virtualmachineclasses` *vm-class-instance-storage*

    ```
    apiVersion: vmoperator.vmware.com/v1alpha2
    kind: VirtualMachineClass
    metadata:
      name: vm-class-instance-storage
    spec:
      hardware:
        cpus: 8
        memory: 64Gi
        devices:
    ...
        instanceStorage:
          storageClass: vsan-direct
          volumes:
          - size: 256Gi
          - size: 512Gi

    ...
    ```

  - El archivo YAML de máquina virtual apunta a la clase de máquina virtual de almacenamiento de instancias adecuada.

Implementar máquinas virtuales con propiedades OVF configurables en vSphere IaaS control plane

Por lo general, cuando un ingeniero de desarrollo y operaciones aprovisiona una máquina virtual en el entorno de vSphere IaaS control plane, una plantilla de OVF incluye detalles codificados de forma rígida, como la configuración básica de red. Sin embargo, es posible que no sepa (y a menudo no pueda) asignar ciertos valores a las propiedades de OVF de la máquina virtual, como los datos de red proporcionados por IPAM, hasta después de crear el recurso personalizado de la máquina virtual. Gracias a la compatibilidad con cadenas de plantillas, no es necesario conocer la información de red de antemano. Puede utilizar plantillas basadas en Golang para rellenar los valores de propiedades de OVF y configurar la pila de red de la máquina virtual.

Procedimiento

1 Asegúrese de que el archivo OVF incluya la entrada `ovf:userConfigurable="true"` para que se configuren todas las propiedades.

Esta entrada permite que el sistema sustituya los marcadores de posición del valor de redes, como servidores de nombres e IP de administración, por datos reales después de que se recopilen los datos.

Utilice el siguiente ejemplo.

```
<Property ovf:key="hostname" ovf:type="string" ovf:userConfigurable="true"
ovf:value="ubuntuguest">
      <Description>Specifies the hostname for the appliance</Description>
</Property>
<Property ovf:key="nameservers" ovf:type="string" ovf:userConfigurable="true"
ovf:value="1.1.1.1, 1.0.0.1">
      <Label>2.2. DNS</Label>
      <Description>A comma-separated list of IP addresses for up to three DNS servers</
Description>
</Property>
<Property ovf:key="management_ip" ovf:type="string" ovf:userConfigurable="true">
      <Label>2.3. Management IP</Label>
      <Description>The static IP address for the appliance on the Management Port Group in
CIDR format (Eg. ip/subnet mask bits). This cannot be DHCP.</Description>
</Property>
```

2 Cree el archivo YAML de máquina virtual con cadenas de plantilla.

Las cadenas de plantilla para los recursos de arranque recopilarán los datos necesarios para rellenar los valores de propiedad de OVF.

Puede utilizar uno de los siguientes métodos para construir cadenas de plantillas.

- Utilice vm-operator-api.

  Para obtener más información, consulte la siguiente página en GitHub: https://github.com/vmware-tanzu/vm-operator/blob/main/api/v1alpha2/virtualmachinetempl_types.go.

  El siguiente es un archivo YAML de ejemplo:

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: template-vm
  namespace: test-ns
  annotations:
    vmoperator.vmware.com/image-supported-check: disable
spec:
  className: best-effort-xsmall
  imageName: vmi-xxxx0000
  powerState: poweredOn
  storageClass: wcpglobal-storage-profile
  vmMetadata:
```

```
    configMapName: template-vm-1
    transport: vAppConfig

---
apiVersion: v1
kind: ConfigMap
metadata:
  name: template-vm-1
  namespace: test-ns
data:
  nameservers: "{{ (index .v1alpha2.Net.Nameservers 0) }}"
  hostname: "{{ .v1alpha2.VM.Name }} "
  management_ip: "{{ (index (index .v1alpha2.Net.Devices 0).IPAddresses 0) }}"
  management_gateway: "{{ (index .v1alpha2.Net.Devices 0).Gateway4 }}"
```

- Utilice las siguientes funciones.

Nombre de función	Firma	Descripción
V1alpha2_FirstIP	func () string	Obtenga la primera dirección IP que no es de bucle invertido de la primera NIC.
V1alpha2_FirstIPFromNIC	func (index int) string	Obtenga la dirección IP que no es de bucle invertido de la i-ésima NIC. Si el índice está fuera de los límites, no se analizará la cadena de plantilla.
V1alpha2_FormatIP	func (IP string, netmask string) string	Formatee una dirección IP con la longitud de red. Una máscara de red puede ser una longitud (por ejemplo, /24) o una notación decimal (por ejemplo, 255.255.255.0). Si la máscara de red de entrada no es válida o es diferente de la máscara predeterminada, no se procesará.
V1alpha2_FormatNameservers	func (count int, delimiter string) string	Formatee el primer recuento de servidores de nombres con un delimitador específico. Un número negativo para el recuento significa todos los servidores de nombres.
V1alpha2_IP	func(IP string) string	Formatee una dirección IP estática con el CIDR de máscara de red predeterminado. Si la IP no es válida, la cadena de plantilla no se procesará.
V1alpha2_IPsFromNIC	func (index int) []string	Enumere todas las IP de la i-ésima NIC. Si el índice está fuera de los límites, no se analizará la cadena de plantilla.

Si utiliza las funciones, el archivo YAML tiene el siguiente aspecto:

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: template-vm
  namespace: test-ns
spec:
  className: best-effort-xsmall
  imageName: vmi-xxxx0000
  powerState: poweredOn
  storageClass: wcpglobal-storage-profile
  vmMetadata:
    configMapName: template-vm-2
    transport: vAppConfig

---
apiVersion: v1
kind: ConfigMap
metadata:
  name: template-vm-2
  namespace: test-ns
data:
  nameservers: "{{ V1alpha2_FormatNameservers 2 \",\" }}"
  hostname: "{{ .v1alpha2.VM.Name }} "
  management_ip: "{{ V1alpha2_FormatIP \"192.168.1.10\" \"255.255.255.0\" }}"
  management_gateway: "{{ (index .v1alpha2.Net.Devices 0).Gateway4 }}"
```

3 Implemente la máquina virtual.

```
kubectl apply -f file_name.yaml
```

Pasos siguientes

Si se produce un error en la personalización, y la máquina virtual no obtiene una dirección IP; inspeccione la máquina virtual mediante la consola web de máquina virtual de vSphere. Consulte Solucionar problemas de máquinas virtuales mediante la consola web de máquina virtual de vSphere.

Supervisar máquinas virtuales disponibles en vSphere IaaS control plane

Como administrador de vSphere, utilice vSphere Client para supervisar una máquina virtual implementada por Desarrollo y operaciones en el entorno de Kubernetes de vSphere IaaS control plane.

No se puede administrar el ciclo de vida de la máquina virtual desde vSphere Client.

Requisitos previos

Un ingeniero de Desarrollo y operaciones implementó una máquina virtual. Consulte *Implementar una máquina virtual independiente en vSphere IaaS control plane*.

Procedimiento

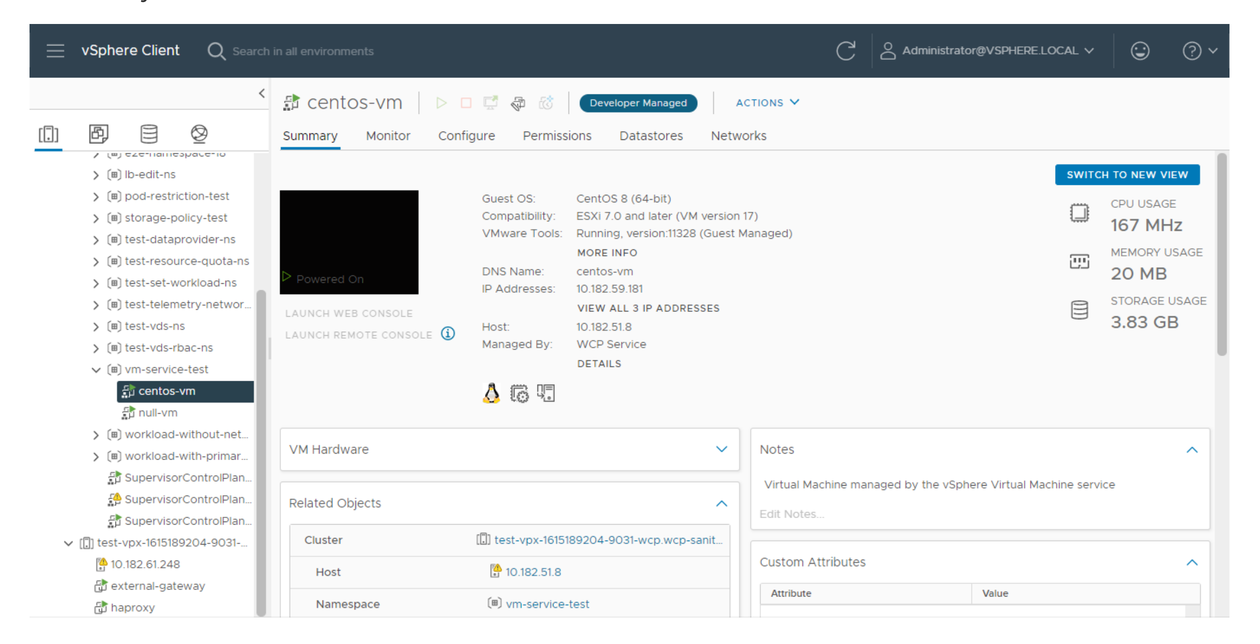
1 En el vSphere Client, desplácese hasta el clúster de host que tiene vSphere IaaS control plane habilitado.

2 En **Espacios de nombres**, expanda el espacio de nombres donde se implementó una máquina virtual.

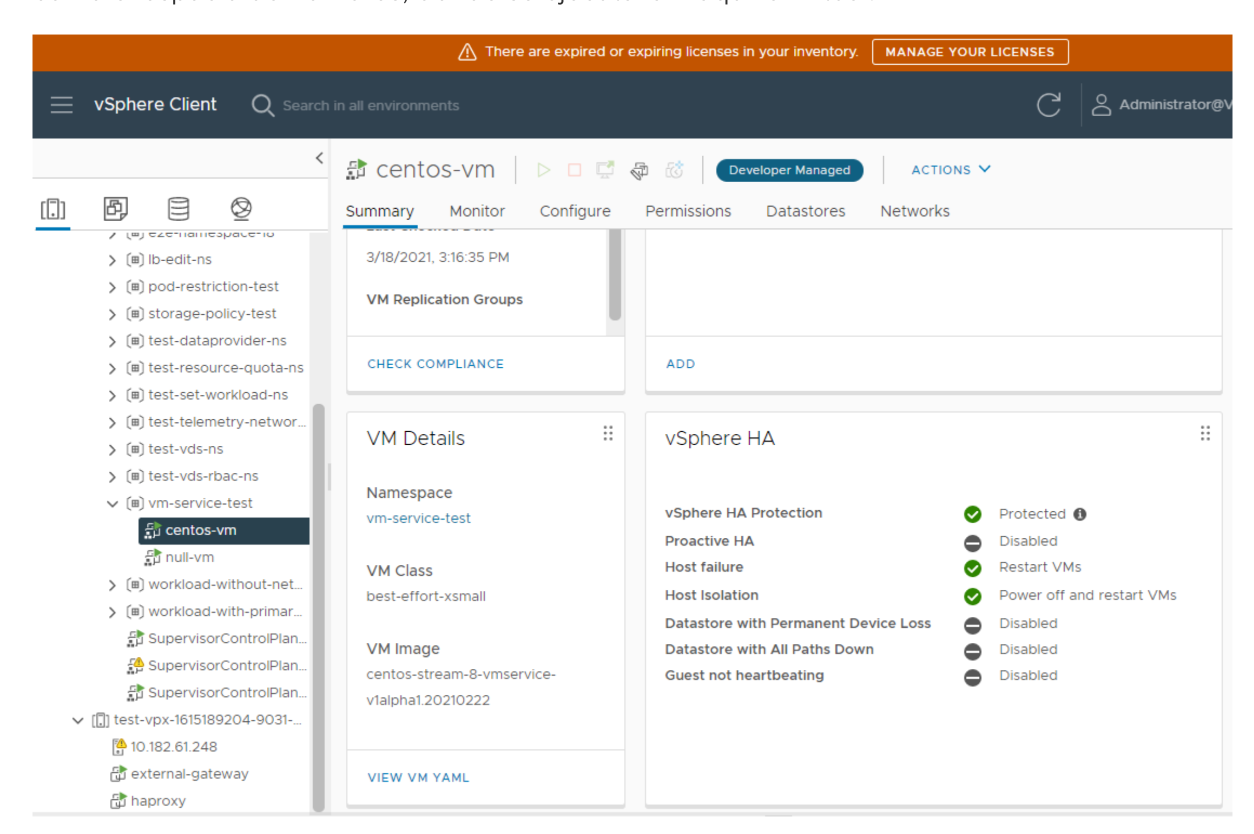
3 Seleccione la máquina virtual que desea ver y haga clic en la pestaña **Resumen**.

Asegúrese de que ve la etiqueta **Administrado por el desarrollador** en la parte superior de la página **Resumen**.

La página muestra información sobre la máquina virtual, incluidos el sistema operativo invitado y las direcciones IP.



4 Haga clic en **Cambiar a nueva vista** en la esquina superior derecha de la página para mostrar detalles adicionales, como la clase de máquina virtual y la imagen de la máquina virtual, así como el espacio de nombres, donde se ejecuta la máquina virtual.



Solucionar problemas de máquinas virtuales mediante la consola web de máquina virtual de vSphere

Como ingeniero de desarrollo y operaciones, puede utilizar la consola web de máquina virtual de vSphere para acceder a las máquinas virtuales problemáticas y solucionar los problemas. El uso de la consola web de máquina virtual puede ser útil cuando no se puede acceder a las máquinas virtuales a través de la red normal, por ejemplo, cuando el sistema operativo invitado no pudo configurar los ajustes de red correctos durante el primer arranque.

La consola web de máquina virtual se vuelve especialmente útil cuando implementan máquinas virtuales con propiedades de OVF configurables. Para obtener más información, consulte Implementar máquinas virtuales con propiedades OVF configurables en vSphere IaaS control plane.

Requisitos previos

Se deben tener permisos de edición o propietario en el espacio de nombres en el que se implementa la máquina virtual problemática. Para obtener más información, consulte Administración de identidad y acceso del plano de control de vSphere IaaS.

Procedimiento

1. Acceda al espacio de nombres en el entorno de Kubernetes.

   Consulte Obtener y utilizar el contexto del Supervisor en vSphere IaaS control plane.

2. Compruebe que la máquina virtual esté implementada.

   ```
   kubectl get vm -n namspace-name
   ```

   El resultado es similar al siguiente:

   ```
   NAME      POWERSTATE       AGE
   vm-name   poweredOn        175m
   ```

3. Obtenga la URL de la consola web de la máquina virtual.

   ```
   kubectl vsphere vm web-console vm-name -n namspace-name
   ```

   Nota El comando devuelve una URL autenticada a la consola web de la máquina virtual como salida. Si no utiliza la URL en un período de tiempo no modificable, establecido en dos minutos, la URL caducará. Después de abrir la URL para conectarse a la página de la consola web, WebMKS controla el tiempo de la sesión y dura más tiempo.

4. Haga clic en la URL y realice las acciones de solución de problemas necesarias para la máquina virtual.

Implementar cargas de trabajo en pods de vSphere

7

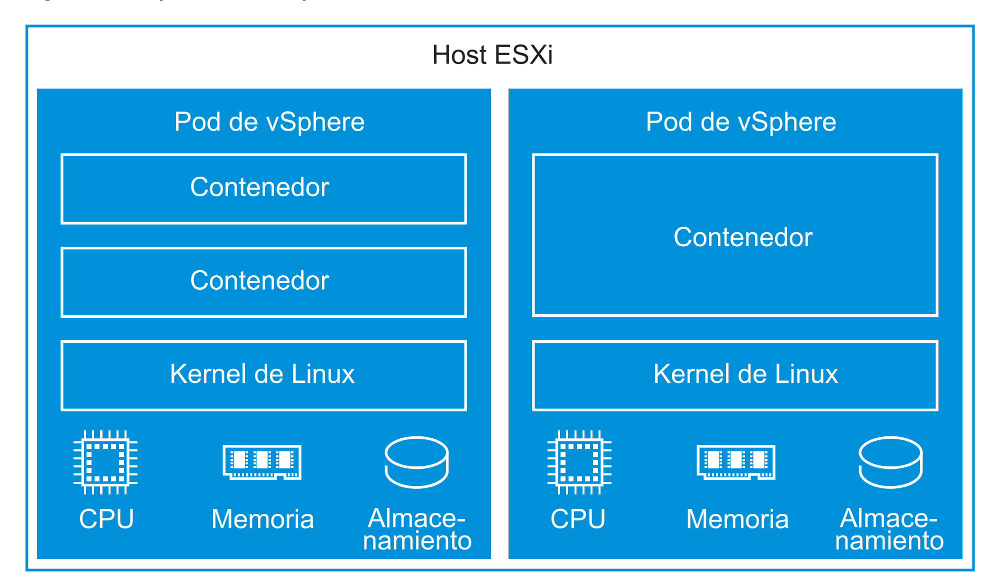
Como ingeniero de desarrollo y operaciones, puede implementar y administrar el ciclo de vida de los pods de vSphere dentro de los límites de recursos de un espacio de nombres de vSphere que se ejecuta en un Supervisor.

Nota Puede implementar pods de vSphere solo en Supervisores que estén configurados con la pila de redes NSX. No se pueden implementar pods de vSphere en Supervisores configurados con la pila de VDS. servicios de supervisor son compatibles con los Supervisores configurados con NSX o VDS e implementan pods de vSphere para su propio uso. Sin embargo, no se puede implementar pods de vSphere para uso genérico en un Supervisor configurado con VDS.

¿Qué es un pod de vSphere?

vSphere IaaS control plane introduce una construcción llamada pod de vSphere, que equivale a un pod de Kubernetes. Una pod de vSphere es una máquina virtual con un tamaño pequeño que ejecuta uno o más contenedores de Linux. Cada pod de vSphere tiene un tamaño preciso para la carga de trabajo que aloja y tiene reservas de recursos explícitas para esa carga de trabajo. Asigna la cantidad exacta de recursos de almacenamiento, memoria y CPU necesarios para la ejecución de la carga de trabajo. Los pods de vSphere solo se admiten con Supervisores que estén configurados con NSX como pila de redes.

Figura 7-1. pods de vSphere



Los pods de vSphere son objetos en vCenter Server y habilitan las siguientes capacidades para las cargas de trabajo:

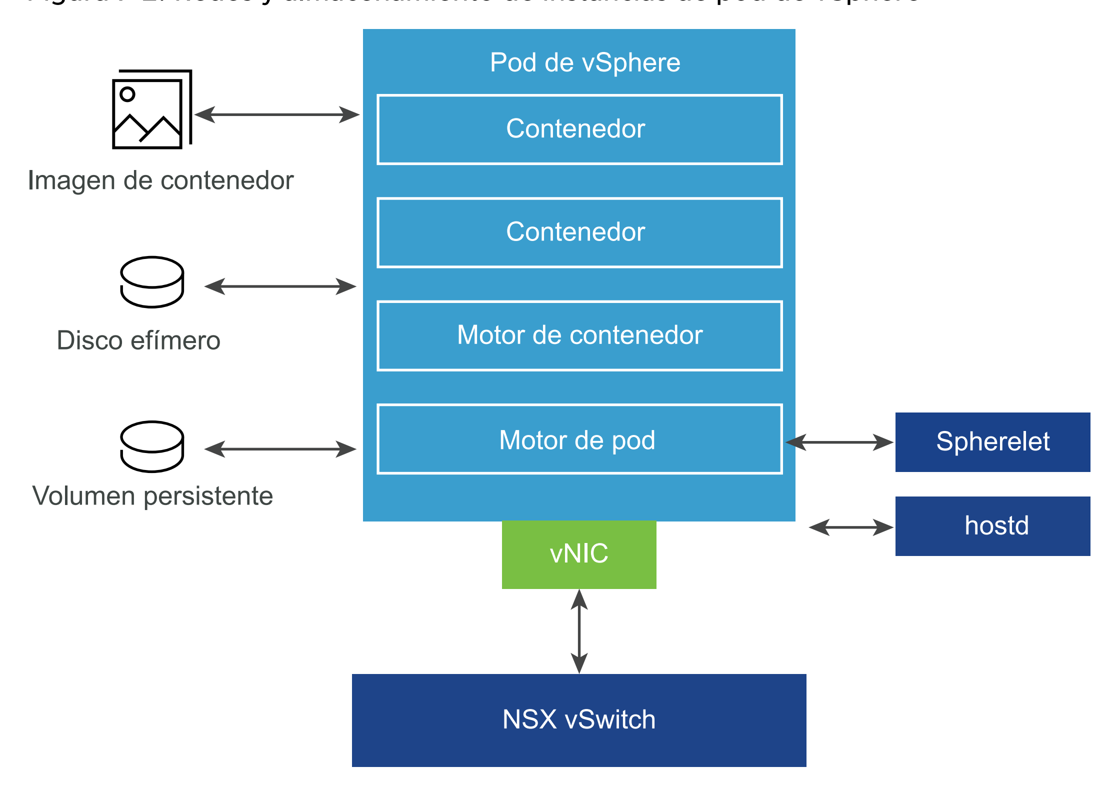
- Aislamiento fuerte. Un pod de vSphere está aislado del mismo modo que una máquina virtual. Cada pod de vSphere tiene su propio kernel único de Linux basado en el kernel utilizado en Photon OS. En lugar de muchos contenedores que comparten un kernel, como en una configuración nativa, en un pod de vSphere, cada contenedor tiene un kernel de Linux único
- Gestión de recursos. vSphere DRS controla la colocación de los pods de vSphere en el Supervisor.
- Alto rendimiento. Los pods de vSphere obtienen el mismo nivel de aislamiento de recursos que las máquinas virtuales, lo que elimina los problemas de vecinos ruidosos a la vez que mantiene el tiempo de inicio rápido y una baja sobrecarga de los contenedores.
- Diagnóstico. Como administrador de vSphere, puede utilizar todas las herramientas de introspección y supervisión que están disponibles con vSphere en las cargas de trabajo.

Los pods de vSphere son compatibles con Open Container Initiative (OCI) y pueden ejecutar contenedores desde cualquier sistema operativo, siempre y cuando estos contenedores también sean compatibles con OCI.

Directrices para la implementación de pods de vSphere

Antes de implementar pods de vSphere, asegúrese de que su entorno cumpla con los siguientes requisitos.

Figura 7-2. Redes y almacenamiento de instancias de pod de vSphere



Espacio de nombres

Sus Supervisores deben tener un espacio de nombres de vSphere configurado con permisos de edición o propietario. Solo los Supervisores de una zona con redes NSX admiten pods de vSphere.

Para crear un Supervisor, consulte Implementar un supervisor de una zona con redes NSX.

Para obtener información sobre cómo crear un espacio de nombres, consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.

Para obtener información sobre la asignación de permisos, consulte Administración de identidades y acceso.

Redes

Para las redes, los pods de vSphere utilizan la topología proporcionada por NSX. Para obtener detalles, consulte Redes de supervisores

Spherelet es un proceso adicional que se crea en cada host. Se trata de un kubelet que se transporta de forma nativa a ESXi y permite que el host ESXi se convierta en parte del clúster de Kubernetes.

Almacenamiento

Los pods de vSphere utilizan tres tipos de almacenamiento en función de los objetos que se almacenen; respectivamente, VMDK efímeros, VMDK de volumen persistente y VMDK de imagen de contenedor.

Como administrador de vSphere, configura directivas de almacenamiento para la colocación de la memoria caché de imagen de contenedor y VMDK efímeros cuando habilita el Supervisor.

En un nivel de espacio de nombres de vSphere, debe configurar las directivas de almacenamiento para la colocación de volúmenes persistentes. Consulte Capítulo 8 Usar almacenamiento persistente con cargas de trabajo de Supervisor en vSphere IaaS control plane para obtener más información sobre los requisitos y conceptos de almacenamiento con vSphere IaaS control plane.

Lea los siguientes temas a continuación:

- Obtener y utilizar el contexto del Supervisor en vSphere IaaS control plane
- Implementar una aplicación en un pod de vSphere en un espacio de nombres de vSphere
- Ampliar una aplicación de pod de vSphere
- Implementar un pod de vSphere confidencial
- Implementación de cargas de trabajo de pod de vSphere en vSphere IaaS control plane

Obtener y utilizar el contexto del Supervisor en vSphere IaaS control plane

Después de que el administrador de vSphere le proporcione la dirección IP del plano de control de Kubernetes en Supervisor, puede iniciar sesión en Supervisor y obtener los contextos a los que tiene acceso. En vSphere IaaS control plane, los contextos corresponden a los espacios de nombres del Supervisor.

Después de iniciar sesión en Supervisor, el complemento de vSphere para kubectl genera el contexto del clúster. En Kubernetes, un contexto de configuración incluye un clúster, un espacio de nombres y un usuario. Puede ver el contexto del clúster en el archivo `.kube/config`. Generalmente, este archivo se denomina `kubeconfig`.

Nota Si ya tiene un archivo `kubeconfig`, este se anexa a cada contexto de clúster. El complemento de vSphere para kubectl respeta la variable de entorno KUBECONFIG que kubectl utiliza. Aunque no es obligatorio, puede que resulte útil definir esta variable antes de ejecutar `kubectl vsphere login ...` para que la información se escriba en un archivo nuevo (en lugar de agregarse al archivo `kubeconfig` actual).

Requisitos previos

- Obtenga las credenciales de vCenter Single Sign-On.
- Obtenga la dirección IP del plano de control de Supervisor.
- Obtenga el nombre de la instancia de espacio de nombres de vSphere.
- Obtenga la confirmación de que tiene permisos **Editar** en espacio de nombres de vSphere.

- Descargar e instalar las herramientas de la CLI de Kubernetes para vSphere. Consulte la documentación de *Instalar y configurar el plano de control de IaaS de vSphere*.
- Para comprobar que el certificado ofrecido por el plano de control de Kubernetes sea de confianza en el sistema, instale la CA de firma como raíz de confianza o agregue el certificado directamente como raíz de confianza. Consulte Configurar el inicio de sesión seguro para clústeres del plano de control IaaS vSphere en la documentación de *Instalar y configurar el plano de control de IaaS de vSphere*.

Procedimiento

1 Para ver la sintaxis y las opciones de los comandos para iniciar sesión, ejecute el siguiente comando.

```
kubectl vsphere login --help
```

2 Para conectarse a Supervisor, ejecute el siguiente comando.

```
kubectl vsphere login --server=<KUBERNETES-CONTROL-PLANE-IP-ADDRESS> --vsphere-username
<VCENTER-SSO-USER>
```

Por ejemplo:

```
kubectl vsphere login --server=10.92.42.13 --vsphere-username administrator@example.com
```

Esta acción crea un archivo de configuración con el token web de JSON (JSON Web Token, JWT) para autenticarse en la API de Kubernetes.

3 Para autenticarse, introduzca la contraseña del usuario.

Después de conectarse a Supervisor, se le mostrarán los contextos de configuración a los que puede acceder. Por ejemplo:

```
You have access to the following contexts:
tanzu-ns-1
tkg-cluster-1
tkg-cluster-2
```

4 Para ver los detalles de los contextos de configuración a los que puede acceder, ejecute el siguiente comando de `kubectl`:

```
kubectl config get-contexts
```

La CLI muestra los detalles de cada contexto disponible.

5 Para cambiar de contexto, utilice el siguiente comando:

```
kubectl config use-context <example-context-name>
```

Pasos siguientes

Para conectarse a un clúster de Tanzu Kubernetes Grid, consulte Conectarse a un clúster de TKG como usuario de vCenter Single Sign-On en *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Implementar una aplicación en un pod de vSphere en un espacio de nombres de vSphere

Puede implementar una aplicación en un espacio de nombres de vSphere de vSphere IaaS control plane. Una vez que se implementa la aplicación, se crea la cantidad correspondiente de instancias de pods de vSphere en el Supervisor del espacio de nombres.

Requisitos previos

- Obtenga de su administrador de vSphere la dirección IP del plano de control de Kubernetes de Supervisor.
- Obtenga su cuenta de usuario en vCenter Single Sign-On.
- Compruebe con el administrador de vSphere si tiene permisos para acceder a los contextos que necesita.

Procedimiento

1 Acceda al espacio de nombres en el entorno de Kubernetes.

   Consulte Obtener y utilizar el contexto del Supervisor en vSphere IaaS control plane.

2 Cambie al contexto en el que desea implementar la aplicación.

   ```
   kubectl config use-context <namespace>
   ```

3 Implemente la aplicación.

   ```
   kubectl apply -f <application name>.yaml
   ```

Ampliar una aplicación de pod de vSphere

Puede realizar una ampliación o una reducción vertical de la cantidad de réplicas para cada aplicación que se ejecute en Supervisor en vSphere IaaS control plane.

Requisitos previos

- Obtenga de su administrador de vSphere la dirección IP del plano de control de Kubernetes de Supervisor.
- Obtenga su cuenta de usuario en vCenter Single Sign-On.
- Compruebe con el administrador de vSphere si tiene permisos para acceder a los contextos que necesita.

Procedimiento

1 Realice la autenticación con Supervisor.

```
kubectl vsphere login --server <control plane load balancer IP address> --vsphere-username
<vSphere user account name>
```

2 Escalado o reducción verticales de una aplicación.

```
kubectl get deployments
kubectl scale deployment <deployment-name> --replicas=<number-of-replicas>
```

Implementar un pod de vSphere confidencial

Con vSphere IaaS control plane, puede ejecutar pods de vSphere confidenciales en un Supervisor. Un pod de vSphere confidencial utiliza una tecnología de hardware que mantiene cifrada la memoria del sistema operativo invitado, lo que la protege del acceso desde el hipervisor.

Puede crear pods de vSphere confidenciales si agrega el estado de cifrado SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) como una mejora de seguridad adicional. SEV-ES impide que los registros de la CPU filtren información en los registros de los componentes como el hipervisor. SEV-ES también puede detectar modificaciones malintencionadas en un estado de registro de la CPU. Para obtener más información sobre el uso de la tecnología SEV-ES en el entorno de vSphere, consulte Proteger máquinas virtuales con virtualización cifrada segura de AMD: estado cifrado en la documentación de *Seguridad de vSphere*.

Requisitos previos

Para habilitar SEV-ES en un host ESXi, el administrador de vSphere debe seguir estas directrices:

- Utilice los hosts que admiten la funcionalidad SEV-ES.
- Utilice ESXi versión 7.0 Update 2 o posteriores.
- Habilite SEV-ES en la configuración de la BIOS del sistema de un ESXi. Consulte la documentación del sistema para obtener más información sobre cómo acceder a la configuración de la BIOS.
- Al hacerlo, introduzca un valor para la opción de **ASID mínimo de estado no cifrado de SEV** que sea igual a la cantidad de máquinas virtuales de SEV-ES y pods de vSphere confidenciales en el host más una. Por ejemplo, si tiene pensado ejecutar 100 máquinas virtuales de SEV-ES y 128 pods de vSphere, introduzca al menos 229. Puede introducir una configuración de hasta 500.

Procedimiento

1 Cree un archivo YAML que contenga los siguientes parámetros.

a En las anotaciones, habilite la función de pods de vSphere confidencial.

```
...
annotations:
        vmware/confidential-pod: enabled
...
```

b Especifique los recursos de memoria para los contenedores.

Asegúrese de establecer las solicitudes de memoria y los límites de memoria en el mismo valor que en este ejemplo.

```
resources:
      requests:
        memory: "512Mi"
      limits:
        memory: "512Mi"
```

Utilice el siguiente archivo YAML como ejemplo:

```
apiVersion: v1
kind: Pod
metadata:
  name: photon-pod
  namespace: my-podvm-ns
  annotations:
    vmware/confidential-pod: enabled
spec:  # specification of the pod's contents
  restartPolicy: Never
  containers:
  - name: photon
    image: wcp-docker-ci.artifactory.eng.vmware.com/vmware/photon:1.0
    command: ["/bin/sh"]
    args:    ["-c", "while true; do echo hello, world!; sleep 1; done"]
    resources:
      requests:
        memory: "512Mi"
      limits:
        memory: "512Mi"
```

2 Inicie sesión en Supervisor.

```
kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user
account name>
```

3 Cambie al espacio de nombres en el que desea implementar la aplicación.

```
kubectl config use-context <namespace>
```

4 Implemente un pod de vSphere confidencial desde el archivo YAML.

```
kubectl apply -f <yaml file name>.yaml
```

Nota Cuando se implementa el pod de vSphere, DRS lo coloca en el nodo ESXi compatible con SEV-ES. Si no hay ningún nodo disponible, el pod de vSphere se marca como con errores.

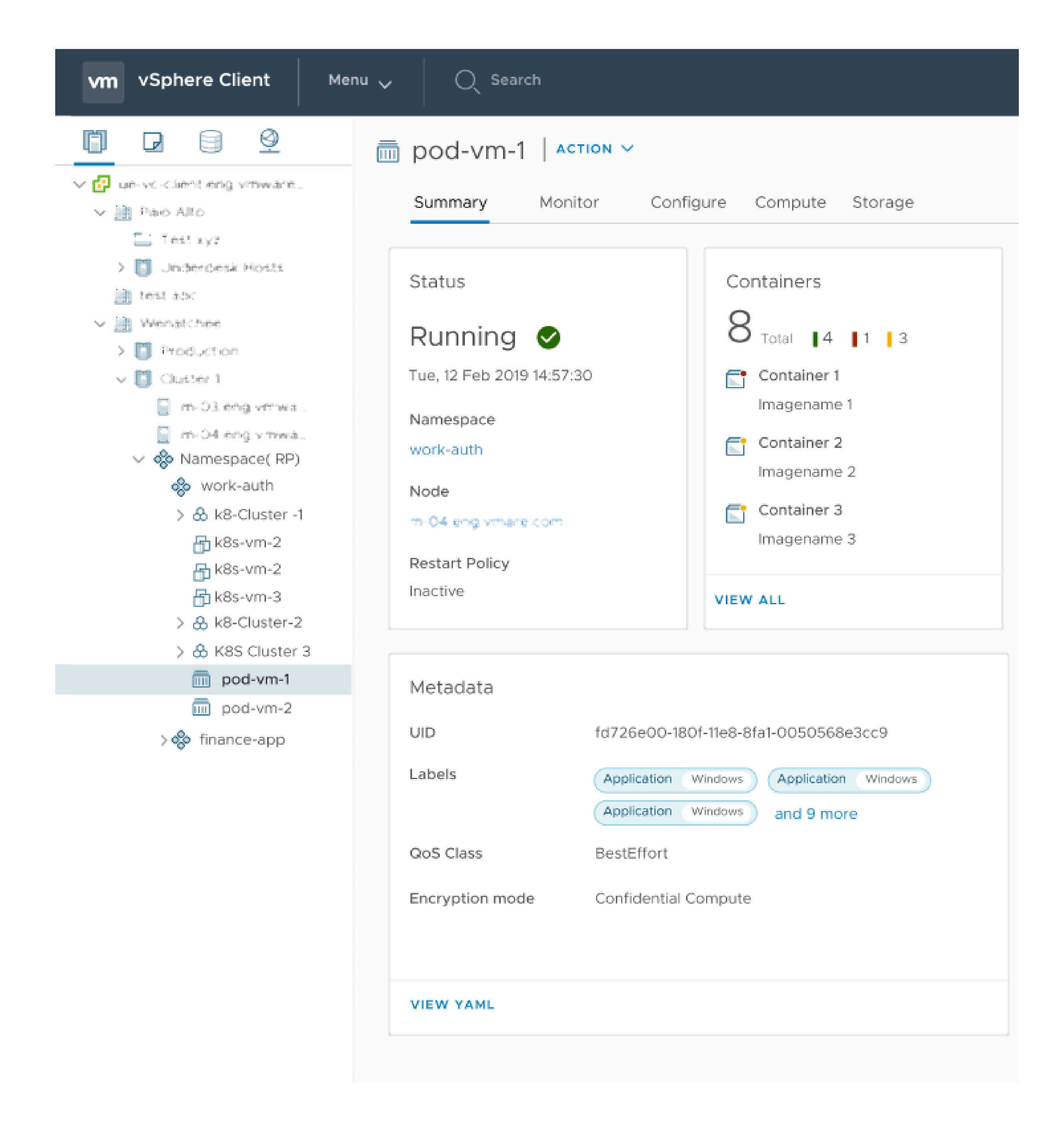
El pod de vSphere confidencial que se inicia proporciona compatibilidad con el cifrado de memoria de hardware para todas las cargas de trabajo que se ejecutan en ese pod.

5 Ejecute el siguiente comando para comprobar que se creó el pod de vSphere confidencial.

```
kubectl describe pod/<yaml name>
```

Pasos siguientes

Un administrador de vSphere puede ver el pod de vSphere confidencial. En el vSphere Client, aparece con la etiqueta **Modo de cifrado: Cálculo confidencial**.



Implementación de cargas de trabajo de pod de vSphere en vSphere IaaS control plane

Este tutorial de ejemplo describe cómo implementar la aplicación de WordPress mediante pods de vSphere en el entorno de vSphere IaaS control plane.

La implementación de WordPress incluye contenedores para el front-end de WordPress y el back-end de MySQL, así como servicios para ambos. También se requieren objetos secretos.

En este tutorial, se utiliza un objeto deployment. En el entorno de producción, debe utilizar StatefulSets para los contenedores de WordPress y MySQL.

Requisitos previos

- Cree un Supervisor de una zona con redes NSX. Solo los Supervisores de una zona con NSX admiten pods de vSphere. Consulte Implementar un supervisor de zona única con redes NSX.
- Cree un espacio de nombres para implementar pods de vSphere. Consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.
- Cree una directiva de almacenamiento, por ejemplo, `vwt-storage-policy` y asígnela al espacio de nombres.
- Descargue las herramientas de la CLI de Kubernetes de vSphere. Consulte Descargar e instalar las herramientas de la CLI de Kubernetes para vSphere.
- Cree los archivos YAML necesarios para este tutorial y compruebe el acceso de la línea de comandos a los archivos.

Categoría	Archivos
Almacenamiento	■ mysql-pvc.yaml ■ namepress-pvc.yaml **Nota** Asegúrese de que los archivos hagan referencia a la clase de almacenamiento correcta.
Secretos	■ regcred.yaml ■ mysql-pass.yaml
Servicios	■ mysql-service.yaml ■ namepress-service.yaml
Implementaciones	■ mysql-deployment-vsphere-pod.yaml ■ namepress-deployment.yaml

Implementar WordPress

Utilice este flujo de trabajo para implementar la aplicación de WordPress mediante pods de vSphere.

Parte 1. Acceder al espacio de nombres

Siga estos pasos para acceder al espacio de nombres.

Procedimiento

1 Inicie sesión en el supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username wcp-user@vsphere.local
```

2 Cambie al espacio de nombres de vSphere.

```
kubectl config use-context VSPHERE-PODS-NAMESPACE
```

3 Compruebe que la directiva de almacenamiento que creó, `vwt-storage-policy`, esté disponible en el espacio de nombres como una clase de almacenamiento.

   Consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere.

Parte 2. Crear PVC de WordPress

Utilice estos comandos para crear PVC de WordPress.

Procedimiento

1 Cree la PVC de MySQL.

```
kubectl apply -f mysql-pvc.yaml
```

2 Cree la PVC de WordPress.

```
kubectl apply -f wordpress-pvc.yaml
```

3 Verifique la PVC.

```
kubectl get pvc,pv
```

Parte 3. Crear secretos

Docker Hub público es el registro de contenedor predeterminado para Kubernetes. Docker Hub ahora limita la extracción de imágenes. Debe tener una cuenta de pago y agregar la clave de cuenta al YAML secreto en el campo `data.dockerconfigjson`.

Procedimiento

1 Cree un secreto de registro de Docker Hub.

```
kubectl apply -f regcred.yaml
```

2 Cree el secreto de contraseña de mysql.

   Se requiere la contraseña de la base de datos MySQL. Dentro del secreto, la contraseña debe estar codificada en base64.

```
kubectl apply -f mysql-pass.yaml
```

3 Verifique los secretos.

```
kubectl get secrets
```

Parte 4. Crear servicios

Siga estos pasos para crear servicios.

Procedimiento

1 Cree el servicio MySQL.

```
kubectl apply -f mysql-service.yaml
```

2 Cree el servicio WordPress.

```
kubectl apply -f wordpress-service.yaml
```

3 Verifique los servicios.

```
kubectl get services
```

Parte 5. Crear implementaciones de pods

Utilice esta tarea para crear implementaciones de pods.

En este tutorial se utilizan objetos de implementación. En el entorno de producción debe utilizar StatefulSets para los contenedores de WordPress y MySQL.

Procedimiento

1 Cree la implementación de MySQL.

```
kubectl apply -f mysql-deployment-vsphere-pod.yaml
```

Nota Cuando se crea una instancia de pod de vSphere, el sistema crea una máquina virtual para los contenedores del pod. De forma predeterminada, la máquina virtual tiene un límite de 512 MB de RAM. El contenedor MySQL requiere más memoria. La especificación de implementación del pod `mysql-deployment-vsphere-pod.yaml` incluye una sección que aumenta la memoria que se otorga a la máquina virtual de pod de vSphere. Si no incluye esta sección, se produce un error en la implementación del pod con una excepción de memoria agotada (OOM). No es necesario aumentar la RAM al implementar un pod MySQL en un clúster de TKG.

2 Cree la implementación de WordPress.

```
kubectl apply -f wordpress-deployment.yaml
```

3 Verifique su implementación.

```
kubectl get deployments
```

Parte 6. Probar WordPress

Siga estos pasos para probar la implementación de WordPress.

Procedimiento

1 Compruebe que todos los objetos se crearon y se están ejecutando.

```
kubectl get pv,pvc,secrets,rolebinding,services,deployments,pods
```

2 Obtenga la dirección IP externa del servicio WordPress.

```
kubectl get service wordpress

NAME        TYPE           CLUSTER-IP    EXTERNAL-IP     PORT(S)        AGE
wordpress   LoadBalancer   10.96.9.180   10.197.154.73   80:30941/TCP   87s
```

3 Desplácese hasta la dirección IP externa.

4 Configure la instancia de WordPress.

Nombre de usuario: administrador

Contraseña: utilice la contraseña segura proporcionada

Ejemplo de archivos YAML para la implementación de WordPress

Utilice estos archivos YAML de ejemplo cuando implemente la aplicación de WordPress con pods de vSphere.

mysql-pvc.yaml

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mysql-pvc
  labels:
    app: wordpress
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: vwt-storage-policy
  resources:
    requests:
      storage: 20Gi
```

namepress-pvc.yaml

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: wordpress-pvc
  labels:
    app: wordpress
spec:
  accessModes:
    - ReadWriteOnce
```

```
  storageClassName: vwt-storage-policy
  resources:
    requests:
      storage: 20Gi
```

regcred.yaml

```
apiVersion: v1
kind: Secret
metadata:
  name: regcred
data:
  .dockerconfigjson: ewoJImF1dGhzIjog....zZG1KcE5WUmtXRUozWpc
type: kubernetes.io/dockerconfigjson
```

mysql-pass.yaml

```
apiVersion: v1
data:
  password: YWRtaW4=  #admin base64 encoded
kind: Secret
metadata:
  name: mysql-pass
```

mysql-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: wordpress-mysql
  labels:
    app: wordpress
spec:
  ports:
    - port: 3306
  selector:
    app: wordpress
    tier: mysql
  clusterIP: None
```

namepress-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
```

```
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
```

mysql-deployment-vsphere-pod.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: wordpress-mysql
  labels:
    app: wordpress
spec:
  replicas: 1
  strategy:
    type: Recreate
  selector:
    matchLabels:
      app: wordpress
      tier: mysql
  template:
    metadata:
      labels:
        app: wordpress
        tier: mysql
    spec:
      containers:
      - image: mysql:5.6
        name: mysql
        #increased resource limits required for this pod vm
        #default pod VM RAM is 512MB; MySQL container needs more
        #without extra RAM OOM error prevents deployment
        #extra RAM not required for Kuberentes cluster
        resources:
          limits:
            memory: 1024Mi
            cpu: 1
        env:
        - name: MYSQL_ROOT_PASSWORD
          valueFrom:
            secretKeyRef:
              name: mysql-pass
              key: password
        ports:
        - containerPort: 3306
          name: mysql
        volumeMounts:
        - name: mysql-persistent-storage
          mountPath: /var/lib/mysql
      volumes:
      - name: mysql-persistent-storage
```

```
        persistentVolumeClaim:
          claimName: mysql-pvc
      imagePullSecrets:
      - name: regcred
```

namepress-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  selector:
    matchLabels:
      app: wordpress
      tier: frontend
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: wordpress
        tier: frontend
    spec:
      containers:
      - image: wordpress:4.8-apache
        name: wordpress
        env:
        - name: WORDPRESS_DB_HOST
          value: wordpress-mysql
        - name: WORDPRESS_DB_PASSWORD
          valueFrom:
            secretKeyRef:
              name: mysql-pass
              key: password
        ports:
        - containerPort: 80
          name: wordpress
        volumeMounts:
        - name: wordpress-persistent-storage
          mountPath: /var/www/html
      volumes:
      - name: wordpress-persistent-storage
        persistentVolumeClaim:
          claimName: wordpress-pvc
      imagePullSecrets:
      - name: regcred
```

Usar almacenamiento persistente con cargas de trabajo de Supervisor en vSphere IaaS control plane

8

Ciertas cargas de trabajo de Kubernetes que desarrollo y operaciones ejecutan en un espacio de nombres en Supervisor requieren almacenamiento persistente para almacenar datos de forma permanente. El almacenamiento persistente puede ser utilizado por pods de vSphere, clústeres de Tanzu Kubernetes Grid, máquinas virtuales y otras cargas de trabajo que se ejecutan en el espacio de nombres.

Para que el almacenamiento persistente esté disponible para el equipo de Desarrollo y operaciones, el administrador de vSphere crea directivas de almacenamiento de máquina virtual que describen diferentes requisitos de almacenamiento y clases de servicios. A continuación, el administrador asigna directivas de almacenamiento y configura los límites de almacenamiento en un nivel de espacio de nombres.

Para comprender cómo funciona vSphere IaaS control plane con el almacenamiento persistente, familiarícese con los conceptos esenciales de Kubernetes, como las clases de almacenamiento, los volúmenes persistentes y las notificaciones de volumen persistente. Para obtener más información, consulte la documentación de Kubernetes en https://kubernetes.io/docs/home/.

Para obtener información sobre cómo se integran los componentes de vSphere IaaS control plane con el almacenamiento, consulte Almacenamiento de supervisor en *Planificación y conceptos del plano de control de IaaS de vSphere*.

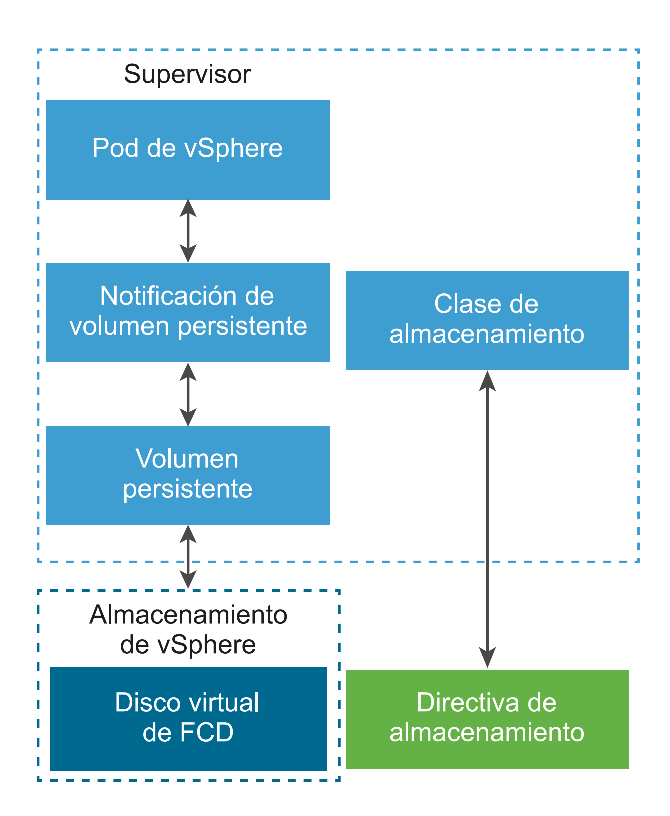
Flujo de trabajo de almacenamiento persistente

El flujo de trabajo para aprovisionar el almacenamiento persistente en vSphere IaaS control plane generalmente incluye las siguientes acciones secuenciales.

Acción	Realizado por	Descripción
Ofrecen recursos de almacenamiento persistentes al equipo de desarrollo y operaciones	Administrador de vSphere	Los administradores de vSphere crean directivas de almacenamiento que describen diferentes requisitos de almacenamiento y clases de servicios. Consulte Crear directivas de almacenamiento para el plano de control de IaaS de vSphere en la documentación de *Instalar y configurar el plano de control de IaaS de vSphere*. A continuación, el administrador asigna las directivas de almacenamiento a un espacio de nombres y establece límites de almacenamiento para el espacio de nombres. Consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.
Crea clases de almacenamiento en el espacio de nombres	vSphere IaaS control plane	Las clases de almacenamiento que coinciden con las directivas de almacenamiento asignadas al espacio de nombres aparecen automáticamente en el entorno de Kubernetes. Si el administrador de vSphere asigna varias directivas de almacenamiento al espacio de nombres, se crea una clase de almacenamiento independiente para cada directiva de almacenamiento. Si utiliza clústeres de Tanzu Kubernetes Grid, cada clúster hereda las clases de almacenamiento del espacio de nombres en el que se aprovisiona el clúster. El equipo de desarrollo y operaciones puede utilizar las clases de almacenamiento para sus necesidades de almacenamiento persistente. Consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere.

Acción	Realizado por	Descripción
Solicita recursos de almacenamiento persistente para una carga de trabajo	DevOps	El equipo de desarrollo y operaciones utiliza las clases de almacenamiento para solicitar recursos de almacenamiento persistentes para una carga de trabajo. La solicitud viene en forma de una notificación de volumen persistente que hace referencia a una clase de almacenamiento específica. Consulte Aprovisionar un volumen persistente dinámico en vSphere IaaS control plane y Implementar una máquina virtual independiente en vSphere IaaS control plane.
Crea un objeto de volumen persistente y un disco virtual persistente coincidente para una carga de trabajo	vSphere IaaS control plane	vSphere IaaS control plane coloca el disco virtual en el almacén de datos que cumple con los requisitos especificados en la directiva de almacenamiento original y su clase de almacenamiento correspondiente. El disco virtual puede montarse mediante una carga de trabajo.
Supervisa volúmenes persistentes	Administrador de vSphere	Mediante vSphere Client, los administradores de vSphere supervisan los volúmenes persistentes y sus discos virtuales de respaldo. También pueden supervisar el cumplimiento de almacenamiento y los estados de mantenimiento de los volúmenes persistentes. Consulte Supervisar volúmenes persistentes en vSphere Client.

A continuación se muestra cómo se crean un objeto de volumen persistente y un disco virtual de FCD persistente coincidente para un pod de vSphere. La notificación de almacenamiento persistente hace referencia a una clase de almacenamiento específica.



Lea los siguientes temas a continuación:

- Mostrar clases de almacenamiento en un espacio de nombres de vSphere
- Aprovisionar un volumen persistente dinámico en vSphere IaaS control plane
- Aprovisionar un volumen persistente estático en vSphere IaaS control plane
- Usar el servicio de archivos de vSAN para crear volúmenes ReadWriteMany en vSphere IaaS control plane
- Expansión de volumen en vSphere IaaS control plane
- Supervisar volúmenes persistentes en vSphere Client
- Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes Grid
- Prácticas recomendadas para usar el almacenamiento persistente en un Supervisor de tres zonas

Mostrar clases de almacenamiento en un espacio de nombres de vSphere

Después de que el administrador de vSphere crea una directiva de almacenamiento y la asigna al espacio de nombres de vSphere de vSphere IaaS control plane, la directiva de almacenamiento se muestra como una clase de almacenamiento de Kubernetes coincidente en el espacio de nombres de vSphere. También se replica en cualquier clúster de Tanzu Kubernetes Grid

disponible. Como ingeniero de desarrollo y operaciones, puede comprobar que la clase de almacenamiento esté disponible.

Su habilidad para ejecutar los comandos depende de sus permisos.

Requisitos previos

Asegúrese de que el administrador de vSphere haya creado una directiva de almacenamiento adecuada y haya asignado la directiva al espacio de nombres de vSphere.

Procedimiento

1 Utilice uno de los siguientes comandos para comprobar que las clases de almacenamiento estén disponibles.

- **kubectl get storageclass**

  Nota Este comando solo está disponible para los usuarios con privilegios de administrador.

  Obtendrá un resultado similar al siguiente: El nombre de la clase de almacenamiento coincide con el nombre de la Directiva de almacenamiento en el lado de vSphere.

```
NAME     PROVISIONER              AGE
silver   csi.vsphere.vmware.com   2d
gold     csi.vsphere.vmware.com   1d
```

- **kubectl describe namespace *namespace_name***

  En el resultado, el nombre de la clase de almacenamiento aparece como parte del parámetro ***storageclass_name*.storageclass.storage.k8s.io/requests.storage**. Por ejemplo:

```
-----------------
Name:                                                             namespace_name
 Resource                                                          Used  Hard
 --------                                                          ---   ---
 silver.storageclass.storage.k8s.io/requests.storage               1Gi
9223372036854775807
 gold.storageclass.storage.k8s.io/requests.storage                 0
9223372036854775807
```

2 Para comprobar la cantidad de espacio de almacenamiento disponible en el espacio de nombres, ejecute el siguiente comando.

kubectl describe resourcequotas -namespace *namespace*

Obtendrá un resultado similar al siguiente:

```
Name:              ns-my-namespace
Namespace:         ns-my-namespace
Resource           Used  Hard
--------           ----  ----
requests.storage   0     200Gi
```

Aprovisionar un volumen persistente dinámico en vSphere IaaS control plane

Las aplicaciones con estado (por ejemplo, bases de datos) guardan datos entre sesiones y requieren volúmenes persistentes para almacenar los datos. Con vSphere IaaS control plane, puede aprovisionar dinámicamente un volumen persistente para la aplicación.

En el entorno de vSphere, los objetos de volúmenes persistentes se respaldan con discos virtuales que residen en almacenes de datos. Los almacenes de datos se representan a través de directivas de almacenamiento. Después de que el administrador de vSphere crea una directiva de almacenamiento (por ejemplo, **`Oro`**) y la asigna a un espacio de nombres en un Supervisor, la directiva de almacenamiento se muestra como una clase de almacenamiento de Kubernetes coincidente en el espacio de nombres de vSphere y los clústeres de Tanzu Kubernetes Grid disponibles.

Como ingeniero de desarrollo y operaciones, puede utilizar la clase de almacenamiento en sus especificaciones de notificación de volúmenes persistentes. Posteriormente, puede implementar una aplicación que utilice almacenamiento de la notificación de volumen persistente. En este ejemplo, el volumen persistente de la aplicación se crea de forma dinámica.

Requisitos previos

Asegúrese de que el administrador de vSphere haya creado una directiva de almacenamiento adecuada y haya asignado la directiva al espacio de nombres.

Procedimiento

1 Acceda al espacio de nombres en el entorno de Kubernetes de vSphere.

   Consulte Obtener y utilizar el contexto del Supervisor en vSphere IaaS control plane.

2 Compruebe que las clases de almacenamiento se encuentren disponibles.

   Consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere.

3 Cree una notificación de volumen persistente (Persistent Volume Claim, PVC).

a Cree un archivo YAML que contenga la configuración de notificación de volumen persistente.

En este ejemplo, el archivo hace referencia a la clase de almacenamiento **gold**.

Para aprovisionar un volumen persistente ReadWriteMany, establezca `accessModes` en `ReadWriteMany`. Consulte Usar el servicio de archivos de vSAN para crear volúmenes ReadWriteMany en vSphere IaaS control plane.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: gold
  resources:
    requests:
        storage: 3Gi
```

b Aplique la notificación de volumen persistente al clúster de Kubernetes.

```
kubectl apply -f pvc_name.yaml
```

Este comando crea de forma dinámica un volumen persistente de Kubernetes y un volumen de vSphere con un disco virtual de respaldo que cumple los requisitos de almacenamiento de la notificación.

c Compruebe el estado de la notificación de volumen persistente.

```
kubectl get pvc my-pvc
```

El resultado muestra que el volumen está enlazado a la notificación de volumen persistente.

```
NAME     STATUS    VOLUME    CAPACITY    ACCESSMODES    STORAGECLASS    AGE
my-pvc   Bound     my-pvc    2Gi         RWO            gold            30s
```

4 Cree un pod que monte el volumen persistente.

a Cree un archivo YAML que incluya el volumen persistente.

El archivo contiene estos parámetros.

```
...
volumes:
    - name: my-pvc
      persistentVolumeClaim:
        claimName: my-pvc
```

b Implemente el pod desde el archivo YAML.

```
kubectl create -f pv_pod_name.yaml
```

c Compruebe que se haya creado el pod.

```
kubectl get pod
```

```
NAME        READY   STATUS    RESTARTS   AGE
pod_name    1/1     Ready     0          40s
```

Resultados

El pod que configuró utilizará el almacenamiento persistente que se describe en la notificación de volumen persistente.

Pasos siguientes

Para supervisar el estado de mantenimiento del volumen persistente, consulte Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes Grid. Para revisar y supervisar el volumen persistente en vSphere Client, consulte Supervisar volúmenes persistentes en vSphere Client.

Aprovisionar un volumen persistente estático en vSphere IaaS control plane

Puede crear estáticamente un volumen de bloque en un clúster de Tanzu Kubernetes Grid mediante una notificación de volumen persistente (PVC) desde Supervisor.

La PVC debe cumplir las siguientes condiciones:

- Estar presente en el mismo espacio de nombres en el que reside el clúster de Tanzu Kubernetes Grid.
- No estar asociada a un pod de vSphere en el Supervisor ni a un pod en cualquier clúster de Tanzu Kubernetes Grid.

Con el aprovisionamiento estático, también puede reutilizar en un nuevo clúster de Tanzu Kubernetes Grid una PVC que ya no necesite otro clúster de Tanzu Kubernetes Grid. Para ello, cambie la `Reclaim policy` del volumen persistente (PV) en el clúster de Tanzu Kubernetes Grid original a `Retain` y, a continuación, elimine la PVC correspondiente.

Siga estos pasos para crear estáticamente una PVC en un nuevo clúster de Tanzu Kubernetes Grid utilizando la información del volumen subyacente de sobra.

Procedimiento

1 Anote el nombre de la PVC original en el Supervisor.

Si vuelve a utilizar la PVC de un clúster de Tanzu Kubernetes Grid antiguo, puede recuperar el nombre de la PVC de `volumeHandle` del objeto PV anterior del clúster de Tanzu Kubernetes Grid.

2 Crear un PV.

En el archivo YAML, especifique los valores de los siguientes elementos:

- Para `storageClassName`, puede introducir el nombre de la clase de almacenamiento que utiliza su PVC en el Supervisor.
- Para `volumeHandle`, introduzca el nombre de PVC que obtuvo en Step 1.

Si está reusando un volumen de otro clúster de Tanzu Kubernetes Grid, elimine los objetos de PVC y PV del clúster de Tanzu Kubernetes Grid anterior antes de crear un PV en el nuevo clúster de Tanzu Kubernetes Grid.

Utilice el siguiente manifiesto de YAML como ejemplo.

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: static-tkg-block-pv
  annotations:
    pv.kubernetes.io/provisioned-by: csi.vsphere.vmware.com
spec:
  storageClassName: gc-storage-profile
  capacity:
    storage: 2Gi
  accessModes:
    - ReadWriteOnce
  persistentVolumeReclaimPolicy: Delete
  claimRef:
    namespace: default
    name: static-tkg-block-pvc
  csi:
    driver: "csi.vsphere.vmware.com"
    volumeAttributes:
      type: "vSphere CNS Block Volume"
    volumeHandle: "supervisor-block-pvc-name"  # Enter the PVC name from the Supervisor.
```

3 Cree un PVC para que coincida con el objeto PV que creó en el paso 2.

Establezca la `storageClassName` en el mismo valor que en el PV.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: static-tkg-block-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 2Gi
  storageClassName: gc-storage-profile
  volumeName: static-tkg-block-pv
```

4 Compruebe que la PVC esté enlazada al PV que creó.

```
$ kubectl get pv,pvc
 NAME                                    CAPACITY   ACCESS MODES   RECLAIM POLICY
STATUS   CLAIM                          STORAGECLASS         REASON   AGE
 persistentvolume/static-tkg-block-pv    2Gi        RWO            Delete
Bound    default/static-tkg-block-pvc   gc-storage-profile            10s

 NAME                                          STATUS   VOLUME                CAPACITY
ACCESS MODES   STORAGECLASS         AGE
 persistentvolumeclaim/static-tkg-block-pvc   Bound    static-tkg-block-pv   2Gi
RWO            gc-storage-profile   10s
```

Usar el servicio de archivos de vSAN para crear volúmenes ReadWriteMany en vSphere IaaS control plane

vSphere IaaS control plane admite volúmenes persistentes en modo ReadWriteMany. Con la compatibilidad de ReadWriteMany, se puede montar un solo volumen simultáneamente mediante varios pods o aplicaciones que se ejecutan en un clúster de TKG. vSphere IaaS control plane utiliza volúmenes de archivos de CNS respaldados por recursos compartidos de archivos de vSAN para los volúmenes persistentes ReadWriteMany. Para utilizar recursos compartidos de vSAN, debe configurar el servicio de archivos de vSAN en el entorno de vSAN y activar la compatibilidad con volúmenes de archivos en el Supervisor.

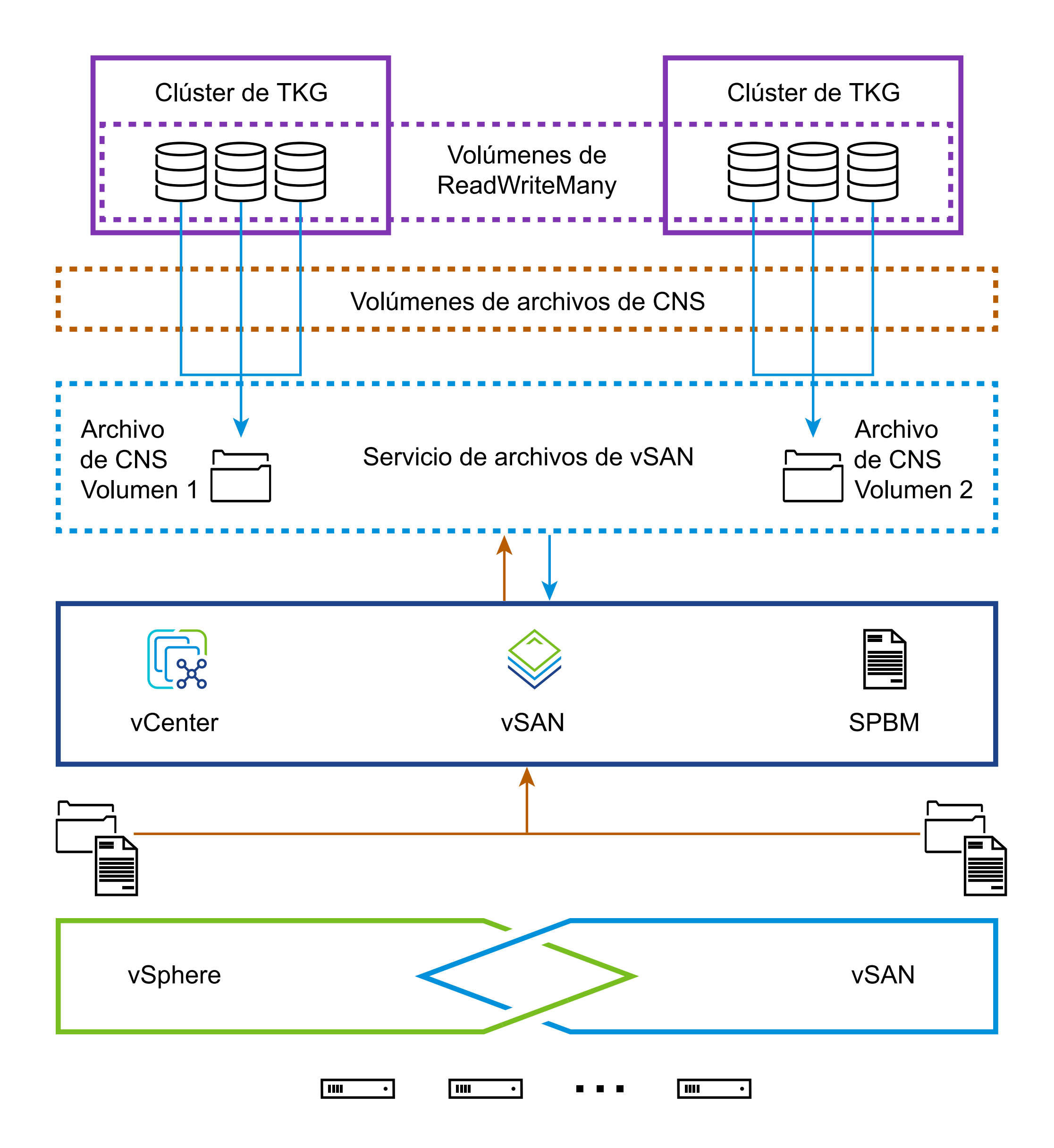
Consideraciones para volúmenes de archivos

Cuando habilite la compatibilidad con volúmenes de archivos para volúmenes persistentes en vSphere IaaS control plane, tenga en cuenta las siguientes consideraciones.

- Los volúmenes de archivos solo se admiten para cargas de trabajo en el clúster de Tanzu Kubernetes Grid. No se admiten para cargas de trabajo, como pods de vSphere y máquinas virtuales de servicio de máquina virtual, en el espacio de nombres Supervisor.

- Cuando se solicita un volumen RWX en Kubernetes, el Servicio de archivos de vSAN crea un recurso compartido de archivos basado en NFS con el tamaño solicitado y la directiva de SPBM adecuada. Se crea un recurso compartido de archivos de vSAN por cada volumen RWX. VMware admite 100 recursos compartidos por clúster de Servicio de archivos de vSAN, lo que significa que no puede tener más de 100 volúmenes RWX.
- Con los clústeres de TKG, utilice la versión 1.22 o posterior de Tkr.

  Para obtener más información, consulte las notas de la versión de VMware Tanzu Kubernetes.
- Cuando habilite la compatibilidad con volúmenes de archivos para vSphere IaaS control plane, tenga en cuenta las posibles debilidades de seguridad:
  - Los volúmenes se montan sin cifrado. Es posible acceder a los datos sin cifrar mientras los datos transitan por la red.
  - Se utilizan listas de control de acceso (ACL) para que los recursos compartidos de archivos aíslen la capacidad de acceso a ellos dentro de un espacio de nombres de supervisor. Puede tener riesgo de suplantación de IP.
- Siga estas directrices para redes:
  - Si utiliza NSX para redes en vSphere IaaS control plane, asegúrese de que el espacio de nombres del Supervisor tenga habilitado el modo NAT. Consulte Crear y configurar un espacio de nombres de vSphere en el Supervisor.
  - Compruebe que el Servicio de archivos de vSAN se pueda enrutar desde la red de carga de trabajo y que no haya ninguna NAT entre la red de carga de trabajo y las direcciones IP del Servicio de archivos de vSAN.
  - Utilice un servidor DNS común para el Servicio de archivos de vSAN y vSphere IaaS control plane.
- Si después de habilitar la compatibilidad con volúmenes de archivos, la desactiva más adelante, los volúmenes persistentes ReadWriteMany existentes que aprovisionó en el clúster no se verán afectados y se podrán seguir usando. No podrá crear nuevos volúmenes persistentes de ReadWriteMany.



Flujo de trabajo para habilitar la compatibilidad con volúmenes de archivos para volúmenes persistentes

Siga este proceso para habilitar la compatibilidad con volúmenes de archivos.

1 Un administrador de vSphere configura un clúster de vSAN con el Servicio de archivos de vSAN configurado.

- Consulte Habilitar el servicio de archivos de vSAN y Configurar el servicio de archivos.
- Para más información sobre los ajustes específicos del entorno con clúster ampliado de vSAN, consulte Servicio de archivos de vSAN con clúster ampliado.

2 Un administrador de vSphere activa la compatibilidad con volúmenes de archivos en Supervisor.

   Consulte Cambiar la configuración de almacenamiento en el supervisor en la documentación de *Instalar y configurar el plano de control de IaaS de vSphere*.

3 Un ingeniero de desarrollo y operaciones aprovisiona un volumen persistente que configura la PVC `accessMode` como `ReadWriteMany`.

Se pueden aprovisionar varios pods con la misma PVC.

Por ejemplo:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: gold
  resources:
    requests:
        storage: 3Gi
```

Expansión de volumen en vSphere IaaS control plane

Como ingeniero de desarrollo y operaciones, puede expandir un volumen de bloques persistentes después de su creación. En vSphere IaaS control plane, ambos tipos de clústeres, tanto Supervisores como Tanzu Kubernetes Grid, admiten la expansión de volúmenes en línea y sin conexión.

Nota Solo puede expandir volúmenes de bloques persistentes. Actualmente, vSphere IaaS control plane no admite la expansión de volúmenes para volúmenes ReadWriteMany.

De forma predeterminada, las clases de almacenamiento que aparecen en el entorno de vSphere IaaS control plane tienen `allowVolumeExpansion` establecido en `true`. Gracias a este parámetro, es posible modificar el tamaño de un volumen en línea y sin conexión.

Se considera que un volumen está sin conexión cuando no está asociado a un nodo o pod. Un volumen en línea es un volumen disponible en un nodo o pod.

El nivel de compatibilidad de la funcionalidad de expansión de volúmenes depende de la versión de vSphere. Puede expandir los volúmenes creados en las versiones anteriores de vSphere cuando actualice el entorno de vSphere a las versiones adecuadas que admitan las ampliaciones.

Al expandir los volúmenes, tenga en cuenta lo siguiente:

- Puede expandir los volúmenes hasta los límites especificados por las cuotas de almacenamiento. vSphere IaaS control plane admite solicitudes de cambio de tamaño consecutivas para un objeto de notificación de volumen persistente.
- Todos los tipos de almacenes de datos, incluidos VMFS, vSAN, vSAN Direct, vVols y NFS, admiten la expansión de volúmenes.
- Puede realizar una expansión de volúmenes para implementaciones o pods independientes.

- Puede cambiar el tamaño de los volúmenes aprovisionados estáticamente en un Supervisor y un clúster de Tanzu Kubernetes Grid si los volúmenes tienen clases de almacenamiento asociadas.
- No se pueden expandir volúmenes que se crean como parte de StatefulSet cuando se utiliza la definición de StatefulSet. Actualmente, Kubernetes no admite esta funcionalidad. Como resultado, se produce un error al intentar expandir los volúmenes aumentando el tamaño de almacenamiento en la definición de StatefulSet.
- Si un disco virtual que crea una copia de seguridad de un volumen tiene instantáneas, no se puede cambiar su tamaño.
- vSphere IaaS control plane no admite la expansión de volúmenes para volúmenes en un árbol o migrados.

Expandir un volumen persistente en modo sin conexión

Se considera que un volumen está sin conexión cuando no está asociado a un nodo o pod. Ambos tipos de clústeres, los clústeres Supervisores y Tanzu Kubernetes Grid, admiten la expansión de volúmenes sin conexión.

Requisitos previos

Asegúrese de actualizar el entorno de vSphere a una versión adecuada que admita la expansión de volúmenes sin conexión.

Procedimiento

1 Cree una notificación de volumen persistente (PVC) con una clase de almacenamiento.

   a Defina una PVC con el siguiente manifiesto de YAML como ejemplo.

   En el ejemplo, el tamaño del almacenamiento solicitado es 1 Gi.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: example-block-pvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: example-block-sc
```

   b Aplique la PVC al clúster de Kubernetes.

```
kubectl apply -f example-block-pvc.yaml
```

2 Aplique una revisión a la PVC para aumentar su tamaño.

Si la PVC no está asociado a un nodo o no lo está usando un pod, utilice el siguiente comando para aplicar una revisión a la PVC. En este ejemplo, el aumento de almacenamiento solicitado es de 2 Gi.

```
kubectl patch pvc example-block-pvc -p '{"spec": {"resources": {"requests": {"storage":
"2Gi"}}}}'
```

Con esta acción se activa una expansión en el volumen asociado a la PVC.

3 Compruebe que el tamaño del volumen haya aumentado.

```
kubectl get pv
NAME                                       CAPACITY ACCESS MODES RECLAIM POLICY STATUS
CLAIM                        STORAGECLASS          REASON AGE
pvc-9e9a325d-ee1c-11e9-a223-005056ad1fc1   2Gi           RWO         Delete      Bound
default/example-block-pvc    example-block-sc              6m44s
```

Nota El tamaño de la PVC no cambia hasta que un pod utiliza la PVC.

El siguiente ejemplo muestra que el tamaño de la PVC no ha cambiado. Si describe la PVC, puede ver la condición `FilesystemResizePending` aplicada en la PVC.

```
kubectl get pvc
NAME                STATUS VOLUME                                     CAPACITY ACCESS
MODES   STORAGECLASS       AGE
example-block-pvc   Bound  pvc-9e9a325d-ee1c-11e9-a223-005056ad1fc1   1Gi
RWO       example-block-sc   6m57s
```

4 Cree un pod para utilizar la PVC.

Cuando el pod utiliza la PVC, se expande el sistema de archivos.

5 Compruebe que el tamaño de la PVC se haya modificado.

```
kubectl get pvc
NAME                STATUS VOLUME                                    CAPACITY ACCESS MODES
STORAGECLASS     AGE
example-block-pvc   Bound  pvc-24114458-9753-428e-9c90-9f568cb25788   2Gi         RWO
example-block-sc 2m12s
```

La condición `FilesystemResizePending` se ha eliminado de la PVC. La expansión del volumen se ha completado.

Pasos siguientes

Un administrador de vSphere puede ver el nuevo tamaño del volumen en vSphere Client. Consulte Supervisar volúmenes persistentes en vSphere Client.

Expandir un volumen persistente en modo en línea

Un volumen en línea es un volumen disponible en un nodo o pod. Como ingeniero de desarrollo y operaciones, puede expandir un volumen de bloque persistente en línea. Ambos tipos de clústeres, Supervisores y Tanzu Kubernetes Grid, admiten la expansión de volúmenes en línea.

Requisitos previos

Asegúrese de actualizar el entorno de vSphere a una versión adecuada que admita la expansión de volúmenes en línea.

Procedimiento

1 Busque la notificación de volumen persistente para cambiar el tamaño.

```
$ kubectl get pv,pvc,pod
NAME                                                        CAPACITY   ACCESS MODES
RECLAIM POLICY   STATUS      CLAIM               STORAGECLASS   REASON   AGE
persistentvolume/pvc-5cd51b05-245a-4610-8af4-f07e77fdc984   1Gi        RWO
Delete           Bound       default/block-pvc   block-sc                4m56s

NAME                              STATUS   VOLUME
CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/block-pvc   Bound    pvc-5cd51b05-245a-4610-8af4-f07e77fdc984
1Gi        RWO            block-sc       5m3s

NAME            READY   STATUS    RESTARTS   AGE
pod/block-pod   1/1     Running   0          26s
```

Tenga en cuenta que el tamaño del almacenamiento que utiliza el volumen es de 1 Gi.

2 Aplique una revisión a la PVC para aumentar su tamaño.

Por ejemplo, aumente el tamaño a 2 Gi.

```
$ kubectl patch pvc block-pvc -p '{"spec": {"resources": {"requests": {"storage":
"2Gi"}}}}'
persistentvolumeclaim/block-pvc edited
```

Con esta acción se activa una expansión en el volumen asociado a la PVC.

3 Compruebe que el tamaño de PVC y PV haya aumentado.

```
$ kubectl get pvc,pv,pod
NAME                              STATUS   VOLUME
CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/block-pvc   Bound    pvc-5cd51b05-245a-4610-8af4-f07e77fdc984
2Gi        RWO            block-sc       6m18s

NAME                                                        CAPACITY   ACCESS MODES
RECLAIM POLICY   STATUS      CLAIM               STORAGECLASS   REASON   AGE
persistentvolume/pvc-5cd51b05-245a-4610-8af4-f07e77fdc984   2Gi        RWO
```

```
Delete           Bound       default/block-pvc   block-sc                6m11s

NAME            READY   STATUS    RESTARTS   AGE
pod/block-pod   1/1     Running   0          101s
```

Pasos siguientes

Un administrador de vSphere puede ver el nuevo tamaño del volumen en vSphere Client. Consulte Supervisar volúmenes persistentes en vSphere Client.

Supervisar volúmenes persistentes en vSphere Client

Cuando los ingenieros de desarrollo y operaciones implementan una aplicación con estado que contiene una notificación de volumen persistente, la vSphere IaaS control plane crea un objeto de volumen persistente y un disco virtual persistente coincidente. Como administrador de vSphere, puede revisar los detalles del volumen persistente en vSphere Client. También puede supervisar el estado de mantenimiento y el cumplimiento de almacenamiento.

Procedimiento

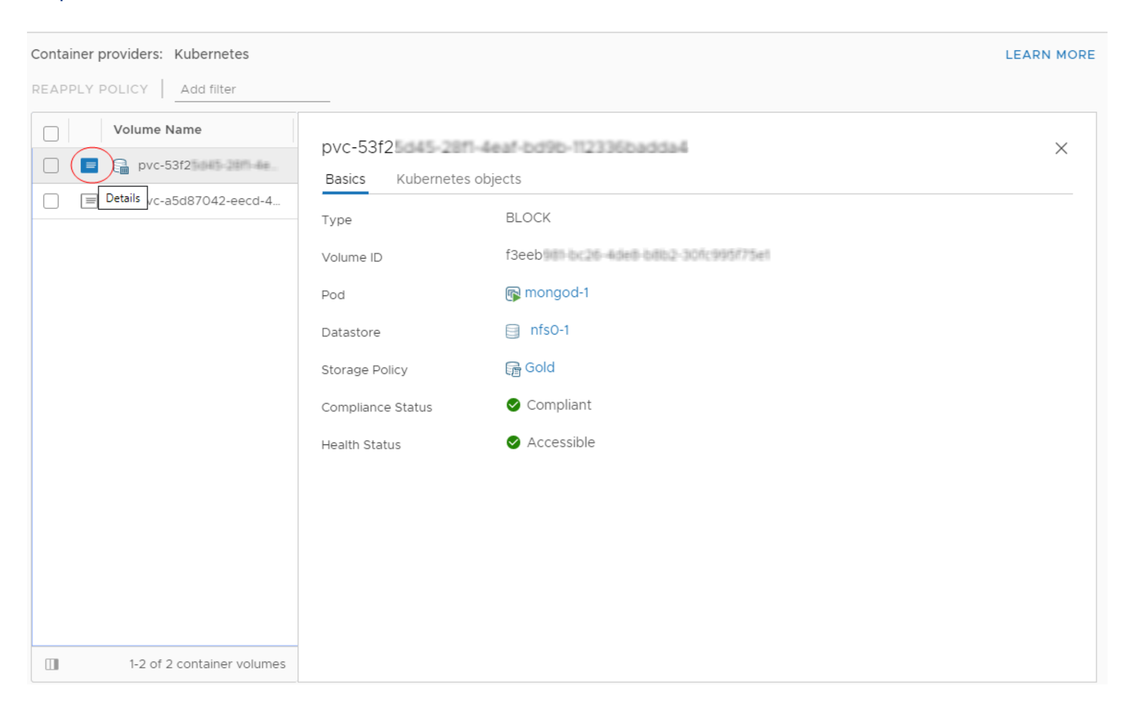
1. En vSphere Client, desplácese hasta el espacio de nombres que tiene los volúmenes persistentes.
   a. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
   b. Haga clic en la pestaña **Espacios de nombres** y seleccione un espacio de nombres de la lista.
2. Haga clic en la pestaña **Almacenamiento** y, a continuación, en **Notificaciones de volumen persistente**.

   En vSphere Client, se enumeran todos los objetos de notificación de volumen persistente y los volúmenes correspondientes disponibles en el espacio de nombres.
3. Para ver los detalles de una notificación de volumen persistente seleccionada, haga clic en el nombre del volumen en la columna **Nombre de volumen persistente**.

4 En la página **Volúmenes contenedores**, compruebe el estado de mantenimiento del volumen y el cumplimiento de la directiva de almacenamiento.

a Haga clic en el icono **Detalles** y alterne entre las pestañas **Conceptos básicos** y **Objetos de Kubernetes** para ver información adicional sobre el volumen persistente de Kubernetes.

Para supervisar el estado de mantenimiento del volumen con el comando `kubectl`, consulte Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes Grid.



b Compruebe el estado de mantenimiento del volumen.

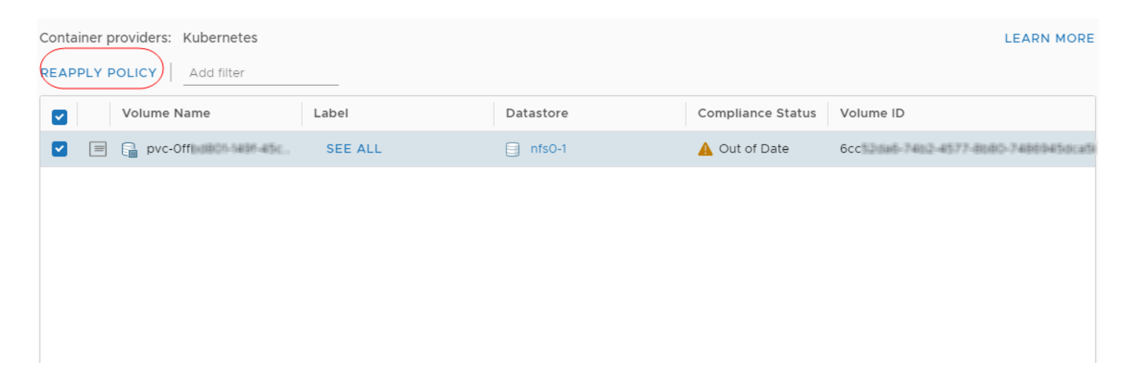
Estado de mantenimiento	Descripción
Accesible	Puede accederse al volumen persistente y está disponible para su uso.
Inaccesible	No puede accederse al volumen persistente y no puede usarse. El volumen persistente se vuelve inaccesible si los hosts que se conectan al almacén de datos no pueden acceder al almacén de datos que almacena el volumen.

c Compruebe el estado de cumplimiento del almacenamiento.

Puede ver una de las siguientes opciones en la columna **Estado de cumplimiento**.

Estado de cumplimiento	Descripción
Conforme	El almacén de datos donde reside el disco virtual de respaldo del volumen tiene las capacidades de almacenamiento que requiere la directiva.
Desactualizado	Este estado indica que la directiva se editó, pero no se comunicaron los nuevos requisitos de almacenamiento al almacén de datos. Para comunicar los cambios, vuelva a aplicar la directiva en el volumen desactualizado.
No compatible	El almacén de datos cumple con los requisitos de almacenamiento especificados, pero actualmente no puede cumplir con la directiva de almacenamiento. Por ejemplo, el estado puede ser de no cumplimiento cuando los recursos físicos del almacén de datos no están disponibles. Puede lograr que el almacén de datos cumpla con los requisitos si realiza cambios en la configuración física del clúster de hosts, por ejemplo, si agrega hosts o discos al clúster. Si los recursos adicionales cumplen con la directiva de almacenamiento, el estado pasará a ser Cumplimiento.
No aplicable	La directiva de almacenamiento hace referencia a las capacidades del almacén de datos no admitidas por el almacén de datos.

d Si el estado de cumplimiento es Desactualizado, seleccione el volumen y haga clic en **Volver a aplicar directiva**.



El estado pasará a ser Conforme.

Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes Grid

Al usar vSphere IaaS control plane, puede comprobar el estado de mantenimiento de un volumen persistente en un estado enlazado.

Para cada volumen persistente en un estado enlazado, el estado de mantenimiento aparece en el campo `Annotations: volumehealth.storage.kubernetes.io/messages:` de la notificación de volumen persistente enlazada al volumen persistente. Existen dos valores posibles para el estado de mantenimiento.

Estado de mantenimiento	Descripción
Accesible	Puede accederse al volumen persistente y está disponible para su uso.
Inaccesible	No puede accederse al volumen persistente y no puede usarse. El volumen persistente se vuelve inaccesible si los hosts que se conectan al almacén de datos no pueden acceder al almacén de datos que almacena el volumen.

Para supervisar el estado de mantenimiento del volumen en vSphere Client, consulte Supervisar volúmenes persistentes en vSphere Client.

Procedimiento

1 Acceda al espacio de nombres en el entorno de vSphere IaaS control plane.

2 Cree una notificación de volumen persistente (Persistent Volume Claim, PVC).

  a Cree un archivo YAML que contenga la configuración de notificación de volumen persistente.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: gold
  resources:
    requests:
        storage: 2Gi
```

  b Aplique la notificación de volumen persistente al clúster de Kubernetes.

```
kubectl apply -f pvc_name.yaml
```

  Este comando crea un volumen persistente de Kubernetes y un volumen de vSphere con un disco virtual de respaldo que cumple con los requisitos de almacenamiento de la notificación.

  c Compruebe si la notificación de volumen persistente está enlazada a un volumen.

```
kubectl get pvc my-pvc
```

  El resultado muestra que la notificación de volumen persistente y el volumen se encuentran enlazados.

```
NAME     STATUS    VOLUME    CAPACITY    ACCESSMODES    STORAGECLASS    AGE
my-pvc   Bound     my-pvc    2Gi         RWO            gold            30s
```

3 Compruebe el estado de mantenimiento del volumen.

Ejecute el siguiente comando para comprobar la anotación del estado del volumen de la notificación de volumen persistente enlazada al volumen persistente.

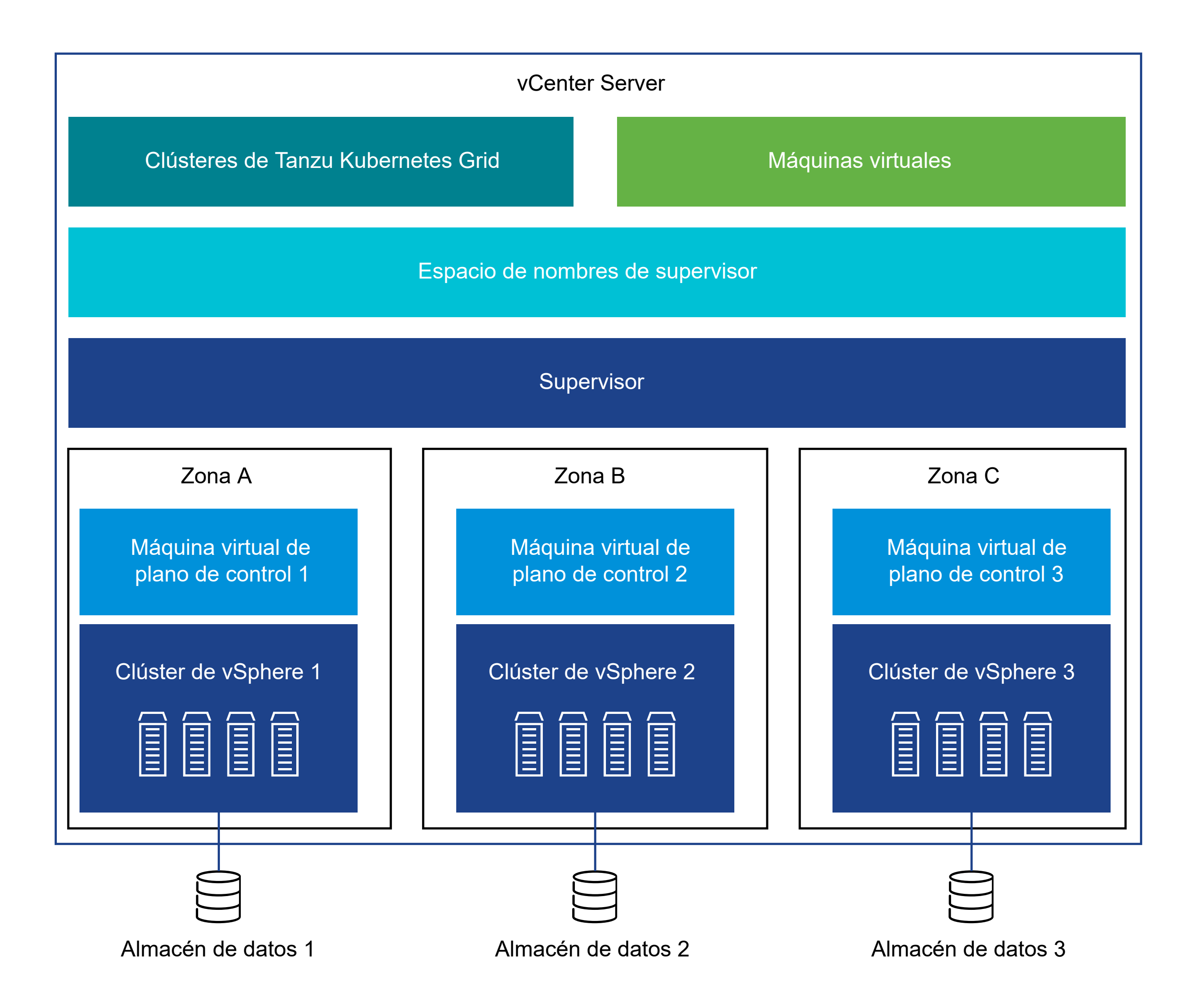
```
kubectl describe pvc my-pvc
```

En los siguientes resultados de ejemplo, el campo `volumehealth.storage.kubernetes.io/messages` muestra el estado de mantenimiento como accesible.

```
Name:          my-pvc
Namespace:     test-ns
StorageClass:  gold
Status:        Bound
Volume:        my-pvc
Labels:        <none>
Annotations:   pv.kubernetes.io/bind-completed: yes
               pv.kubernetes.io/bound-by-controller: yes
               volume.beta.kubernetes.io/storage-provisioner: csi.vsphere.vmware.com
               volumehealth.storage.kubernetes.io/messages: accessible
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:      2Gi
Access Modes:  RWO
VolumeMode:    Filesystem
```

Prácticas recomendadas para usar el almacenamiento persistente en un Supervisor de tres zonas

Un Supervisor de tres zonas en vSphere IaaS control plane admite el almacenamiento de zonas, donde un almacén de datos se comparte entre todos los hosts de una sola zona.



Cuando prepare recursos de almacenamiento para el Supervisor de tres zonas, tenga en cuenta las siguientes consideraciones:

- No es necesario que el almacenamiento de las tres zonas sea del mismo tipo. Sin embargo, tener un almacenamiento uniforme en los tres clústeres proporciona un rendimiento coherente.
- Para el espacio de nombres en el Supervisor de tres zonas, utilice una directiva de almacenamiento que sea compatible con el almacenamiento compartido en cada uno de los clústeres. La directiva de almacenamiento debe tener reconocimiento de topología.
- No elimine las restricciones de topología de la directiva de almacenamiento después de asignarla al espacio de nombres.
- No monte almacenes de datos de zonas en otras zonas.
- Un Supervisor de tres zonas no admite los siguientes elementos:
  - Volúmenes entre zonas

- Volúmenes de archivos de vSAN (volúmenes ReadWriteMany)
- Aprovisionamiento de volúmenes estáticos mediante la API de registrar volumen
- Cargas de trabajo que utilizan la plataforma de persistencia de datos de vSAN
- pod de vSphere
- Clústeres ampliados de vSAN
- Máquinas virtuales con vGPU y almacenamiento de instancias

Crear una directiva de almacenamiento para un supervisor de tres zonas

Para poder utilizar el almacenamiento persistente, las cargas de trabajo que se ejecutan en el Supervisor de tres zonas deben tener acceso a las clases de almacenamiento con topología de zona. Para que estas clases de almacenamiento estén disponibles, el administrador de vSphere crea directivas de almacenamiento con reconocimiento de topología y las asigna al espacio de nombres.

El espacio de nombres del Supervisor de tres zonas impide que se asignen directivas de almacenamiento que no reconozcan la topología.

Para obtener información sobre cómo habilitar Supervisor de tres zonas, consulte Habilitar un supervisor de tres zonas.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a En el menú **Inicio**, haga clic en **Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

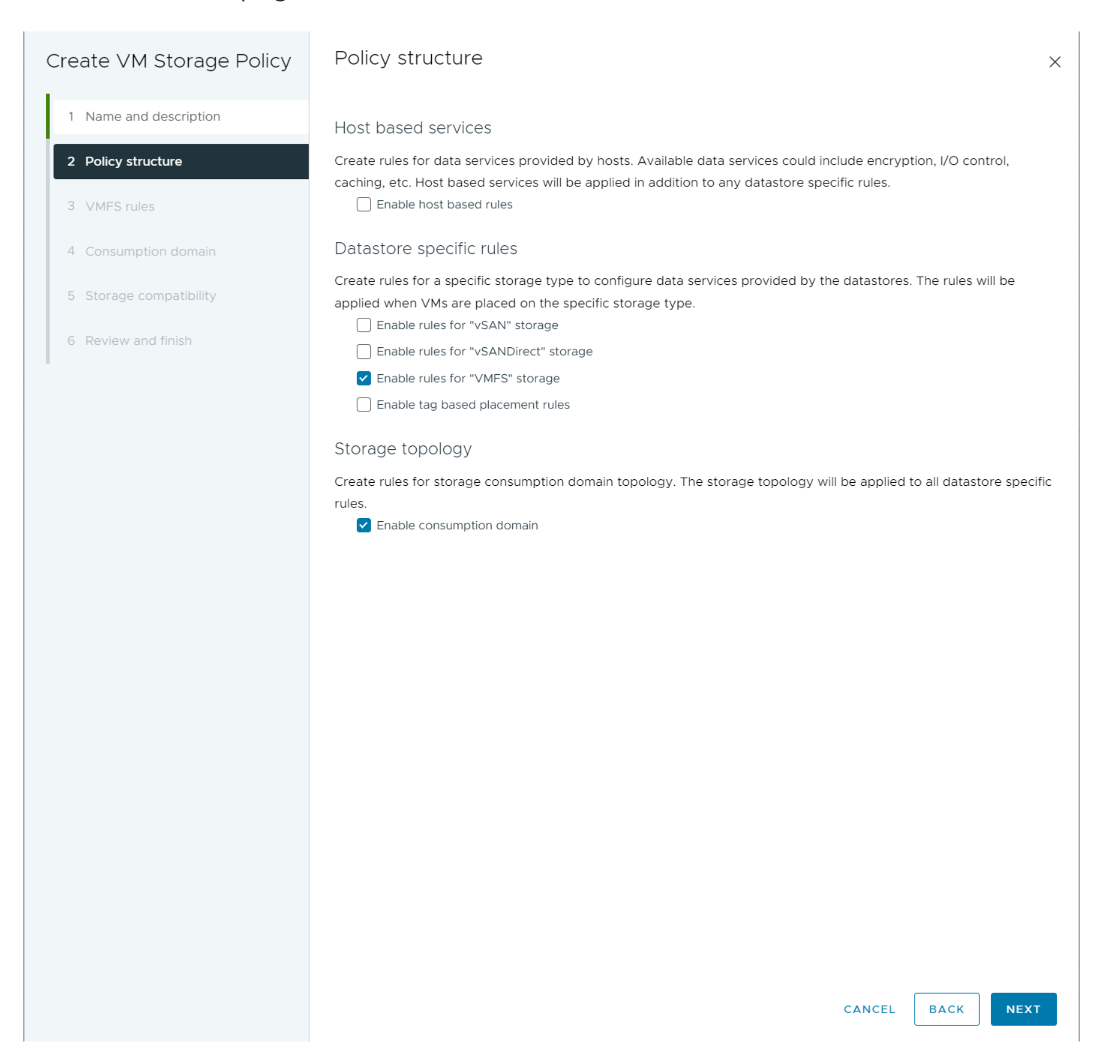
   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 Siga las indicaciones a la página **Estructura de directivas**.

4 En **Topología de almacenamiento**, seleccione **Habilitar dominio de consumo** y siga las indicaciones a la página **Dominio de consumo**.



5 En la página **Dominio de consumo**, especifique el tipo de topología de almacenamiento.

Opción	Descripción
Zonal	El almacén de datos se comparte entre todos los hosts de una sola zona.

Crear PVC en un supervisor de tres zonas

Cuando se crea una PVC dinámica en un Supervisor de tres zonas, puede especificar en qué zonas se debe aprovisionar el volumen.

Procedimiento

- Para controlar la colocación de la zona de PVC, utilice la anotación `csi.vsphere.volume-requested-topology` de Kubernetes en el archivo YAML de PVC.

  Precaución Este parámetro es necesario cuando se crea una PVC directamente en Supervisor. Sin embargo, no incluya anotaciones de zona en la PVC que cree para un clúster de Tanzu Kubernetes Grid. Si lo hace, la PVC no funcionará.

  ```
  apiVersion: v1
  kind: PersistentVolumeClaim
  metadata:
    name: svcpvc4
    annotations:
      csi.vsphere.volume-requested-topology: '[{"topology.kubernetes.io/zone":"zone-1"},
  {"topology.kubernetes.io/zone":"zone-2"},{"topology.kubernetes.io/zone":"zone-3"}]'
  spec:
    accessModes:
      - ReadWriteOnce
    resources:
      requests:
        storage: 10Mi
    storageClassName: zonal2
  ```

  Cuando se especifican las tres zonas, el volumen se crea en zona-1, zona-2 o zona-3.

Pasos siguientes

Para obtener información sobre la implementación de aplicaciones con estado en clústeres de Tanzu Kubernetes Grid, consulte Implementar una aplicación StatefulSet en zonas de vSphere con asociación de volumen de vinculación retrasada.

Instalar y configurar Harbor y Contour en vSphere IaaS control plane

9

Consulte cómo implementar y configurar Harbor y Contour como servicios de supervisor en el entorno de vSphere IaaS control plane. Harbor es un registro nativo en la nube de código abierto que puede utilizar con las cargas de trabajo que se ejecutan en vSphere IaaS control plane. Contour es un controlador de entrada para Kubernetes que funciona implementando el proxy Envoy como proxy inverso y equilibrador de carga. Contour admite actualizaciones de configuración dinámica de forma predeterminada, a la vez que mantiene un perfil ligero.

Puede utilizar Contour como servicio de supervisor como controlador de entrada para las aplicaciones. Contour también es un requisito para ejecutar servicio de supervisor de Harbor.

Nota servicios de supervisor se admiten en Supervisores de clúster único que se ejecutan en pilas de redes VDS o NSX. No se pueden implementar servicios de supervisor en Supervisores de tres zonas.

Harbor como servicio de supervisor proporciona las siguientes capacidades y funciones:

- La versión más reciente del registro de código abierto de Harbor.
- Acceso a Harbor con las cuentas raíz y de administrador.
- Paridad de características completa con el registro de Harbor ascendente.
- Acceso a Harbor a través del ingreso (Contour) mediante DNS.

Nota Cuando se implementan, servicios de supervisor de Harbor y Contour crean pods de vSphere en los espacios de nombres de vSphere creados para estos servicios. Estos pods de vSphere son necesarios para que los servicios funcionen. No se pueden implementar pods de vSphere fuera de servicios de supervisor en una instancia de Supervisor que se ejecuta en la pila de redes VDS o en una instancia de Supervisor de tres zonas. Solo puede implementar pods de vSphere para uso genérico en un Supervisor de clúster único implementado con NSX.

Lea los siguientes temas a continuación:

- Instalar Contour como servicio de supervisor en vSphere IaaS control plane
- Instalar y configurar Harbor en un Supervisor en vSphere IaaS control plane
- Migrar imágenes del registro integrado a Harbor en vSphere IaaS control plane

Instalar Contour como servicio de supervisor en vSphere IaaS control plane

Consulte cómo instalar Contour como servicio de supervisor en los Supervisores del entorno de vSphere IaaS control plane. Una vez instalado, puede utilizar Contour como controlador de entrada para sus aplicaciones. Contour también es un requisito para ejecutar Harbor como un servicio de supervisor.

Requisitos previos

- Compruebe que tenga el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega los servicios.
- Compruebe que haya actualizado a vCenter Server 8.0a o una versión posterior. Los servicios de supervisor de Harbor y Contour son compatibles con vCenter Server 8.0a y versiones posteriores.

Procedimiento

1 Vaya a la sección Versiones de Contour del repositorio de Supervisor-Services y descargue los siguientes archivos:

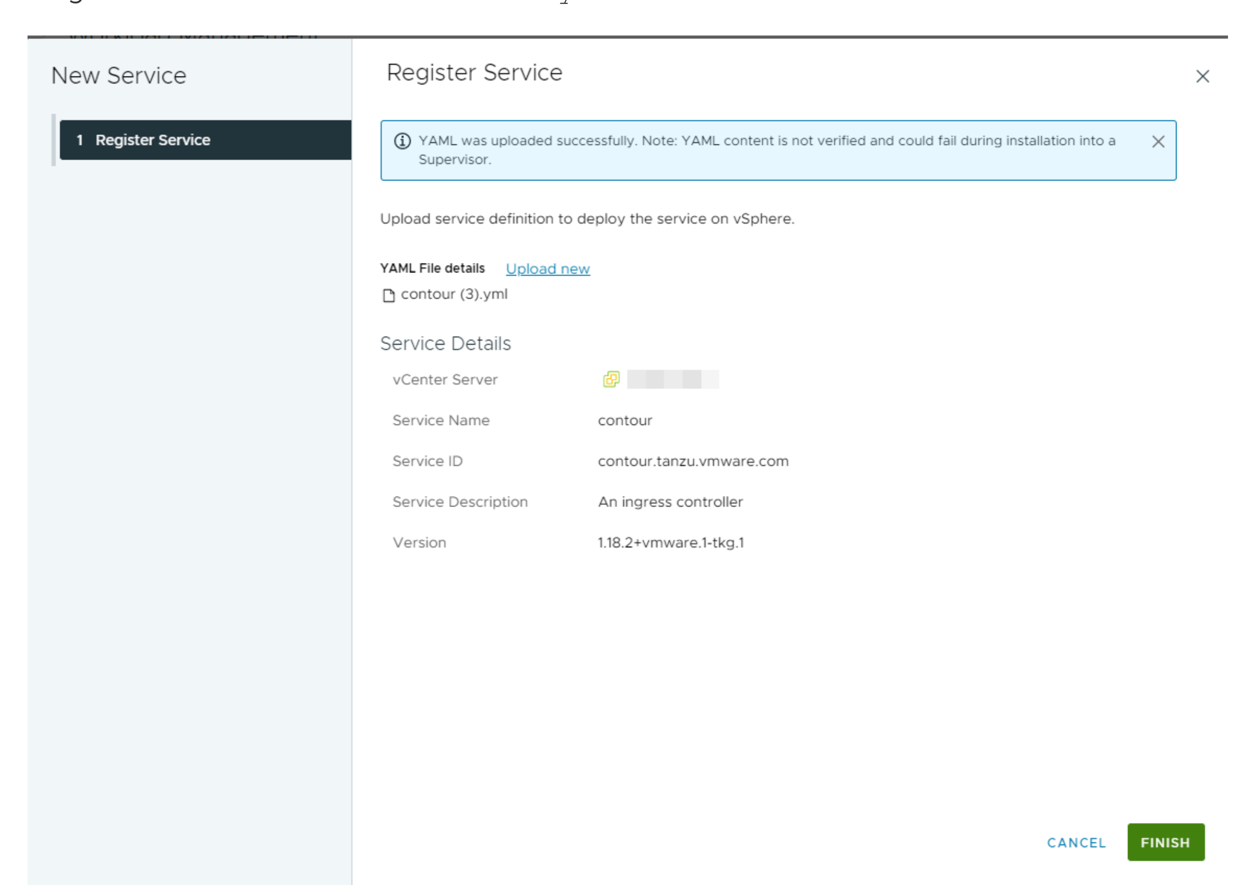
   - La definición del servicio de Contour, el vínculo se denomina `Contour vX.X.X.`. Por ejemplo, `Contour 1.18.2`
   - El archivo de configuración de Contour, el vínculo denominado `valores para vX.X.X`. Por ejemplo, `valores 1.18.2`

   Los archivos resultantes son:

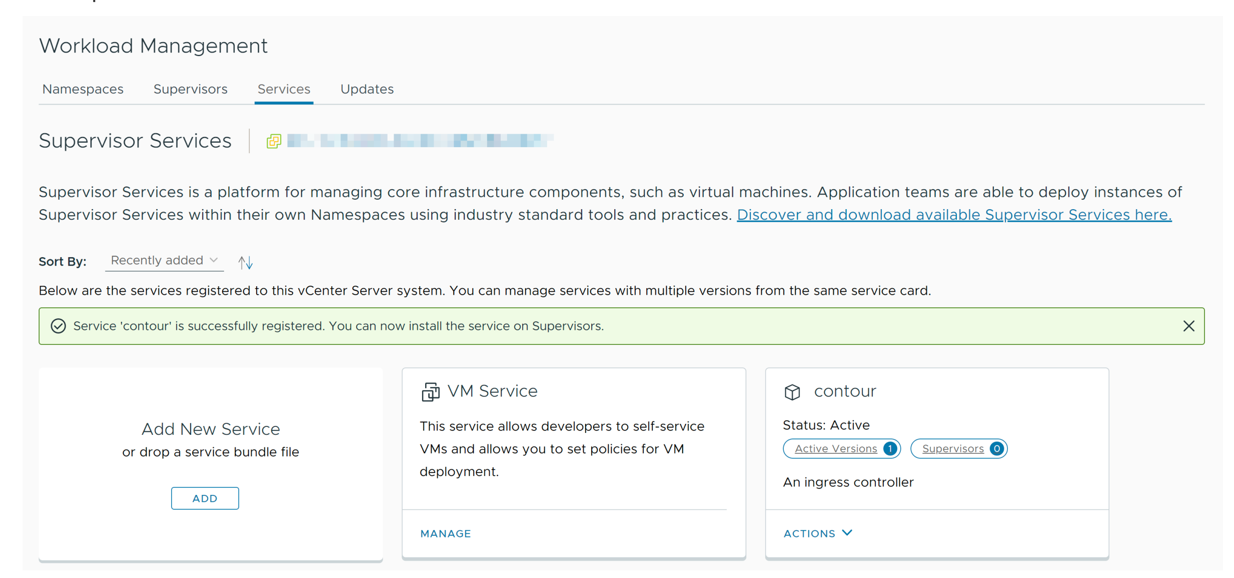
   - `contour.yml`
   - `contour-data-values.yml`

2 En vSphere Client vaya a **Administración de cargas de trabajo** y seleccione **Servicios**.

3 Para implementar el operador de servicios de Contour, haga clic en **Agregar nuevo servicio** y cargue la definición de servicio `contour.yml`.



Cuando el operador de Contour se implementa correctamente, su tarjeta de servicio aparece en la pestaña **Servicios**.



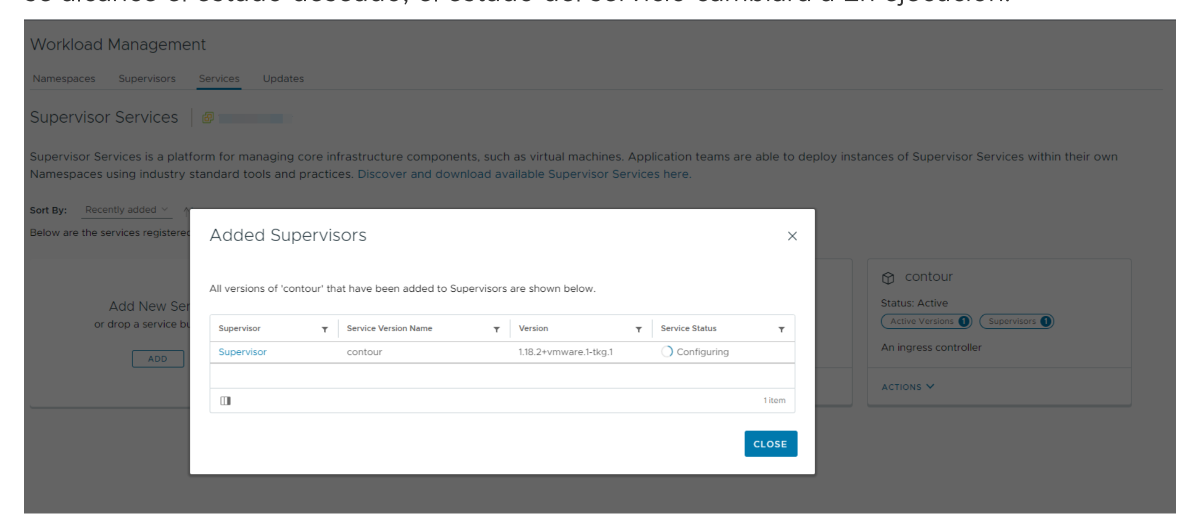
4 Ahora que el operador de Contour está implementado, puede instalar el servicio de supervisor en los Supervisores.

a En la tarjeta de servicio **Contour**, seleccione **Acciones > Instalar en supervisores**.

b Seleccione un Supervisor y, en **Configuración del servicio YAML**, copie y pegue el contenido del archivo `contour-data-values.yml` sin cambiar los valores predeterminados.

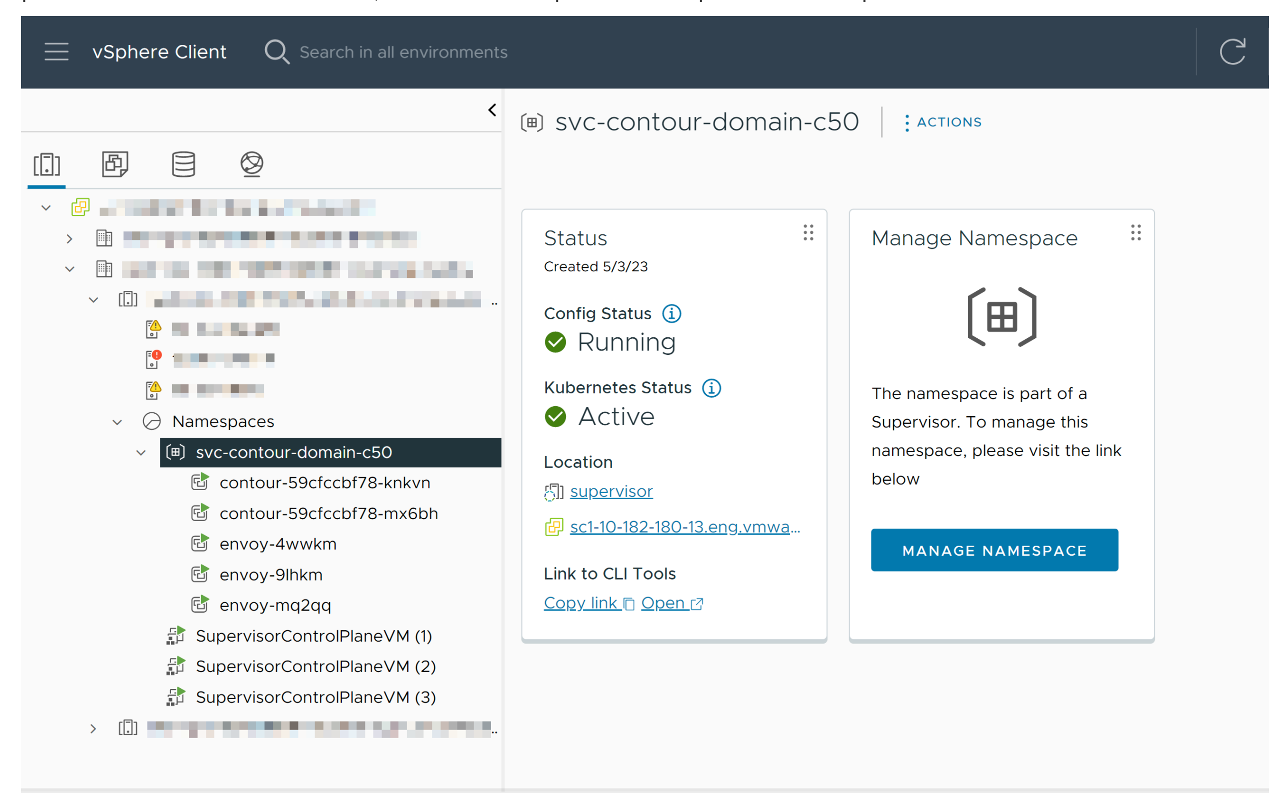
c Haga clic en **Aceptar**.

Una vez que comience la instalación, puede realizar un seguimiento haciendo clic en el campo **Supervisores** en la tarjeta de servicio de Contour. Puede que demore unos segundos hasta que el número junto a **Supervisores** se incremente. El estado del servicio será Configurando hasta que se alcance el estado deseado. Cuando se alcance el estado deseado, el estado del servicio cambiará a En ejecución.

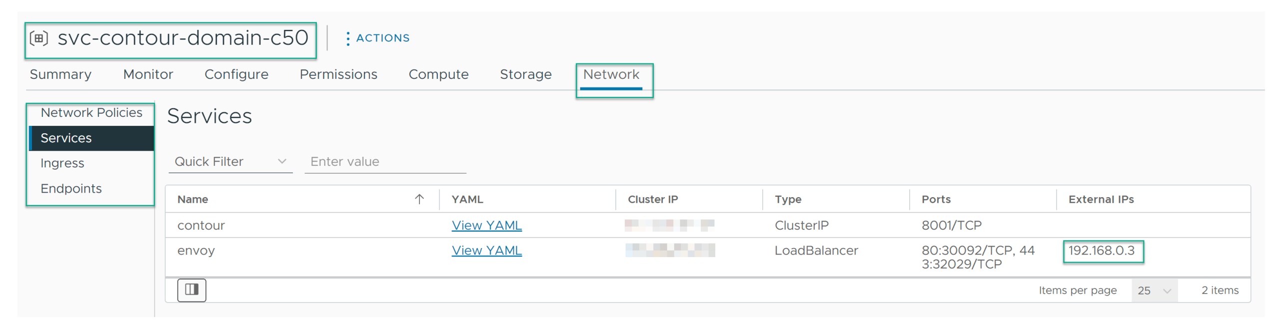


Resultados

Una vez que Contour está instalado, se implementa un espacio de nombres de vSphere creado para la instancia de servicio, así como los pods de vSphere correspondientes:



También puede ver la dirección IP del servicio Envoy que puede asignar a nombres de dominio en un servidor DNS externo que esté configurado con el Supervisor. Puede utilizar las asignaciones para proporcionar la entrada a las aplicaciones a través de Contour. Puede ver la dirección IP de Envoy desde la opción **Red** del espacio de nombres de vSphere de Contour:



Pasos siguientes

Si desea utilizar Harbor como servicio de supervisor para proporcionar un registro para las cargas de trabajo, puede instalar el servicio y configurarlo para usarlo con las cargas de trabajo. Consulte Instalar y configurar Harbor en un Supervisor en vSphere IaaS control plane.

Instalar y configurar Harbor en un Supervisor en vSphere IaaS control plane

Revise cómo instalar y configurar Harbor como un servicio de supervisor. A continuación, podrá utilizar Harbor como registro de cargas de trabajo que se ejecutan en clústeres de Tanzu Kubernetes Grid y pods de vSphere. Harbor necesita a Contour como controlador de entrada, por lo que primero debe instalar el servicio de supervisor de Contour y luego instalar Harbor.

Instalar Harbor como un servicio de supervisor

Harbor se instala como un servicio de supervisor mediante la opción **Administración de cargas de trabajo** en vSphere Client.

Requisitos previos

- Compruebe que haya actualizado a vCenter Server 8.0a o una versión posterior. Los servicios de supervisor de Harbor y Contour son compatibles con vCenter Server 8.0a y versiones posteriores.
- Compruebe que tenga el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega los servicios.
- Instale Contour como servicio de supervisor en el mismo Supervisor en el que desea instalar Harbor. Consulte Instalar Contour como servicio de supervisor en vSphere IaaS control plane.
- Designe y utilice un FQDN para acceder a la interfaz de usuario del administrador de Harbor.

Procedimiento

1 Vaya a la sección Versiones de Harbor del repositorio de Supervisor-Services y descargue los siguientes archivos:

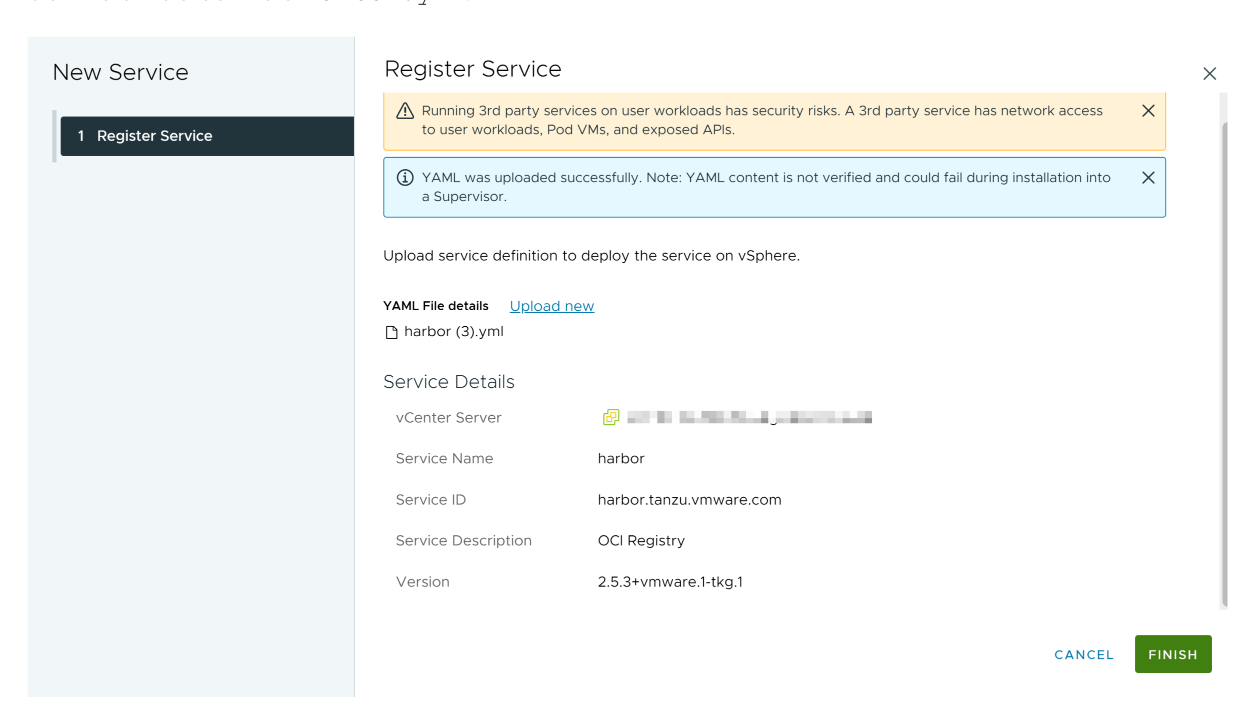
   - La definición del servicio de Harbor, el vínculo se denomina `Harbor vX.X.X`. Por ejemplo, `Harbor 2.5.3`
   - El archivo de configuración de Harbor, el vínculo denominado `valores para vX.X.X`. Por ejemplo, `valores 2.5.3`

   Los archivos resultantes se ven así:

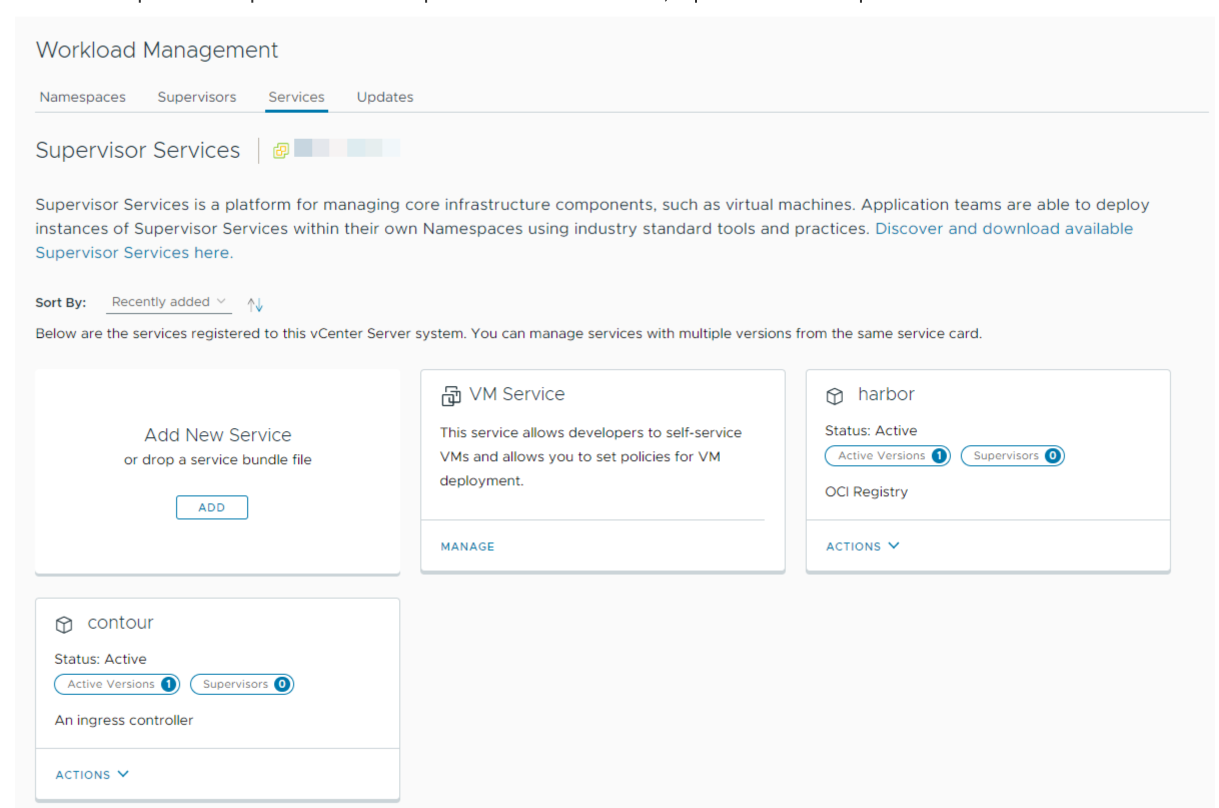
   - `harbor.yml`
   - `harbor-data-values.yml`

2 En vSphere Client vaya a **Administración de cargas de trabajo** y seleccione **Servicios**.

3 Para implementar el operador de Harbor, haga clic en **Agregar nuevo servicio** y cargue la definición de servicio `harbor.yml`.



Una vez que se implementa el operador de Harbor, aparece en la pestaña **Servicios**:



4 Ahora que el operador de Harbor está implementado, puede instalar el servicio de supervisor en el mismo Supervisor en el que se ejecuta Contour.

a Abra el archivo `harbor-data-values.yml` y edite las propiedades según sea necesario.

Propiedad	Valor	Descripción
`hostname: myharbor.com` `  https: 443`	FQDN	Cambie el FQDN que designó para acceder a la interfaz de usuario del administrador de Harbor.
`tlsCertificate:` `  tlsSecretLabels:` `{"managed-by": "vmware-` `vRegistry"}`	**Nota** No cambiar	Este valor es necesario para que funcione la integración de TKG.
`harborAdminPassword:` `Harbor12345`	Cambio opcional	La contraseña de Harbor que se usa durante la instalación. Puede cambiarla a través de la interfaz de usuario de administrador de Harbor, una vez que se haya instalado el servicio.
`secretKey:` `0123456789ABCDEF`	Cadena de 16 caracteres	La clave secreta utilizada para el cifrado. Debe ser una cadena de 16 caracteres.
`database:` `  password: change-it`	Una contraseña segura	Una contraseña inicial usada para la base de datos Postgres.
`core:` `  replicas:` `  secret: change-it` `  xsrfKey:` `0123456789ABCDEF0123456789` `ABCDEF` `jobservice:` `  replicas: 1` `  secret: change-it` `registry:` `  replicas:` `  secret: change-it`	Cadenas para los secretos y una cadena de clave XSRF de 32 caracteres	Cambie para configurar sus propios secretos.
`persistence:` `  persistentVolumeClaim:` `    registry:` `storageClass: "insert-` `storage-class-name-here"` `      subPath: ""` `      accessMode:` `ReadWriteOnce` `      size: 10Gi` `    jobservice:` `storageClass: "insert-` `storage-class-name-here"`	Nombre de clase de almacenamiento	Las directivas de almacenamiento que se utilizarán como clases de almacenamiento para aprovisionar PVC en el registro de Harbor, el servicio de trabajo, la base de datos, etc. Establezca cada una de las propiedades en función de las directivas de almacenamiento existentes que están disponibles en su entorno. Cambie el nombre de la directiva de

Propiedad	Valor	Descripción
<pre> subPath: "" accessMode: ReadWriteOnce size: 1Gi database: storageClass: "insert- storage-class-name-here" subPath: "" accessMode: ReadWriteOnce size: 1Gi redis: storageClass: "insert- storage-class-name-here" subPath: "" accessMode: ReadWriteOnce size: 1Gi trivy: storageClass: "insert- storage-class-name-here" subPath: "" accessMode: ReadWriteOnce size: 5Gi</pre>		almacenamiento por un nombre de clase de almacenamiento válido reemplazando todas las letras mayúsculas por minúsculas, así como reemplazando todos los símbolos y espacios "_" por un guion, "-". Por ejemplo, modifique la **`directiva de almacenamiento`** a **`harbor-storage-policy`**.
<pre>network: ipFamilies: ["IPv4"]</pre>	**Nota** No cambiar	No se admite IPv6.

b Vuelva a **Administración de cargas de trabajo > Servicios** y, en la tarjeta de servicio **Harbor**, seleccione **Acciones > Instalar en supervisores**.

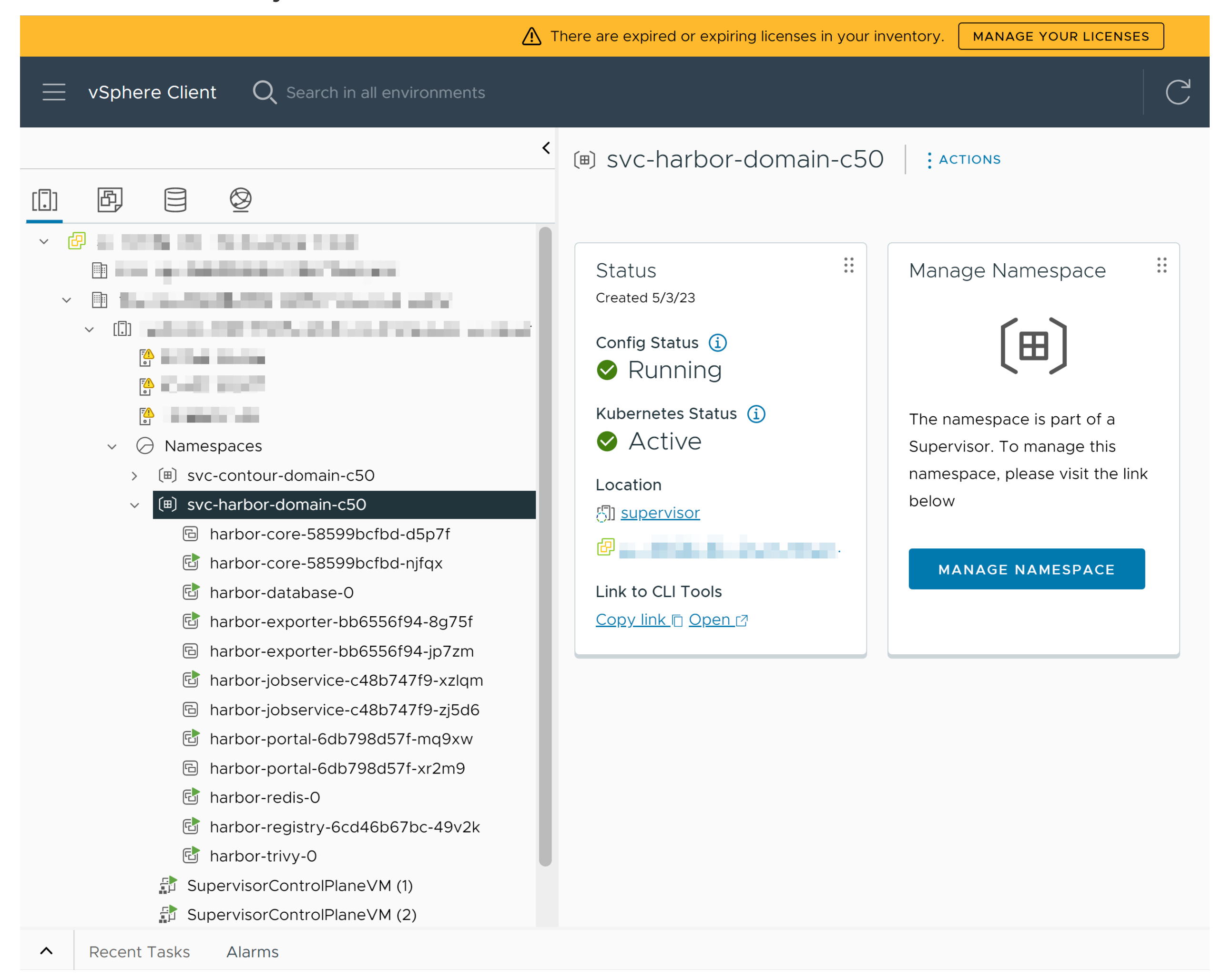
c Seleccione el Supervisor en el que se ejecuta Contour y, en **Configuración de servicio YAML** copie y pegue el contenido del archivo `harbor-data-values.yml` modificado.

d Haga clic en **Aceptar**.

Una vez que comience la instalación, puede realizar un seguimiento haciendo clic en el campo **Supervisores** en la tarjeta de servicio de Harbor. Puede que demore unos segundos hasta que el número junto a **Supervisores** se incremente. El estado del servicio será Configurando hasta que se alcance el estado deseado. Cuando se alcance el estado deseado, el estado del servicio cambiará a En ejecución.

Resultados

Puede ver los espacio de nombres de vSphere y los pods de vSphere creados para Harbor desde la vista **Hosts y clúster**.

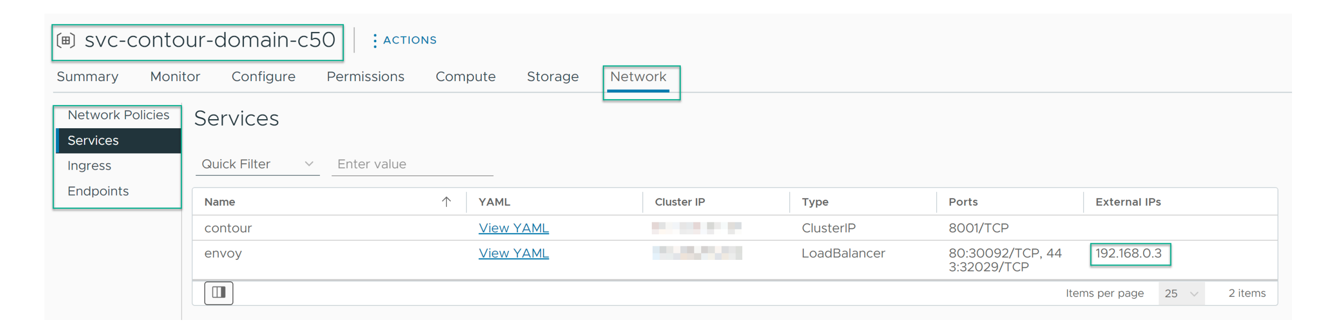


Asignar el FQDN de Harbor a la dirección IP de entrada de Envoy

Después de que se instale satisfactoriamente Harbor, incluya un registro de la asignación de FQDN de Harbor a la dirección IP de entrada de Envoy en un servidor DNS externo que esté configurado con el Supervisor.

Los clústeres de Tanzu Kubernetes Grid, los pods de vSphere y el Supervisor deben poder resolver el FQDN de Harbor para poder extraer imágenes del registro.

Para localizar la dirección IP de entrada de Envoy, desplácese hasta el espacio de nombres de Contour, seleccione **Red** y, a continuación, seleccione **Servicios**:



Establecer la confianza con el servicio de supervisor de Harbor

Una vez que Harbor esté instalado, debe configurar la confianza entre el Supervisor y Harbor para utilizarlo como registro de los pods de vSphere. Los clústeres de Tanzu Kubernetes Grid que están en la misma instancia de Supervisor que Harbor tienen la confianza establecida con Harbor automáticamente. Para utilizar Harbor como registro para clústeres de Tanzu Kubernetes Grid que se ejecutan en diferentes Supervisores, debe configurar la confianza entre Harbor y estos clústeres de Tanzu Kubernetes Grid.

Establecer la confianza entre Harbor y Supervisor

Para establecer la confianza entre Harbor y el Supervisor:

1 Extraiga la CA de Harbor de la interfaz de usuario de Harbor o mediante el secreto TLS en el plano de control del Supervisor. Puede obtener el archivo `ca.cert` en la interfaz de usuario del administrador de Harbor en **Administración > Configuración > Certificado raíz del registro > Descargar**.

2 Agregue la CA de Harbor al configMap de `image-fetcher-ca-bundle` en el espacio de nombres `kube-system`. Debe haber iniciado sesión con una cuenta administrativa de vCenter Single Sing-On y tener permiso para editar `image-fetcher-ca-bundle`.

   a Configure la variable de entorno KUBE_EDITOR como se describe aquí:

   b Edite el ConfigMap mediante el siguiente comando:

   ```
   kubectl edit configmap image-fetcher-ca-bundle -n kube-system
   ```

   c Anexe el contenido del archivo de Harbor `caca.cert` al ConfigMap debajo del certificado de Supervisor existente. Asegúrese de no cambiar el certificado de Supervisor.

   ```
   apiVersion: v1
   data:
     ca-bundle: |-
       -----BEGIN CERTIFICATE-----
       MIIC/jCCAeagAwIBAgIBADANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwprdWJl
       ...
       qB72tWi8M5++h2RGcVash0P1CUZOHkpHxGdUGYv1Z97W189dT2OTn3iXqn8d1JAK
       aF8=
       -----END CERTIFICATE-----
       -----BEGIN CERTIFICATE-----
   ```

```
    MIIDKDCCAhCgAwIBAgIQBbUsj7mqXXC5XRhqqU3GiDANBgkqhkiG9w0BAQsFADAU
    ...
    5q7y87vOLTr7+0MG4O01zK0dJYx2jVhZlsuduMYpfqRLLewVl0eGu/6vr2M=
    -----END CERTIFICATE-----
kind: ConfigMap
metadata:
  creationTimestamp: "2023-03-15T14:28:34Z"
  name: image-fetcher-ca-bundle
  namespace: kube-system
  resourceVersion: "713"
  uid: 6b7611a0-25fa-40f7-b4f5-e2a13bd0afe3
```

d Guarde las ediciones realizadas en el archivo. Como resultado, kubectl notifica:

```
configmap/image-fetch-ca-bundle edit
```

Establecer la confianza entre Harbor y el clúster de Tanzu Kubernetes Grid que se ejecuta en Supervisores diferentes a Harbor

Los clústeres de Tanzu Kubernetes Grid que se ejecutan en Supervisores diferentes al que tiene instalado Harbor deben tener conectividad de red con Harbor. Estos clústeres de Tanzu Kubernetes Grid deben poder resolver el FQDN de Harbor.

Para establecer la confianza entre Harbor y los clústeres de Tanzu Kubernetes Grid, extraiga la CA de Harbor de la interfaz de usuario de Harbor o mediante el secreto TLS en el plano de control del Supervisor y, a continuación, siga los pasos que se indican en Integrar un clúster de TKG 2 con un registro de contenedor privado.

Migrar imágenes del registro integrado a Harbor en vSphere IaaS control plane

Si utiliza el registro de Harbor integrado con su instancia del Supervisor, puede migrar las imágenes del registro integrado en el registro de Harbor que instaló como servicio de supervisor.

Requisitos previos

- Compruebe que los servicios de supervisor Contour y Harbor estén instalados en el Supervisor.
- Compruebe que el DNS que utiliza con el Supervisor incluya una entrada del FQDN de Harbor que está asignado a la IP de entrada del servicio Envoy.
- Compruebe que se haya establecido la confianza entre el Supervisor y Harbor. Si los clústeres de Tanzu Kubernetes Grid que se ejecutan en los Supervisores hacen referencia a imágenes que no son las que se ejecutan en Harbor, compruebe que exista confianza entre estos clústeres de Tanzu Kubernetes Grid y Harbor.

Procedimiento

1 Inicie sesión en el Supervisor como usuario de vCenter Single Sign-On.

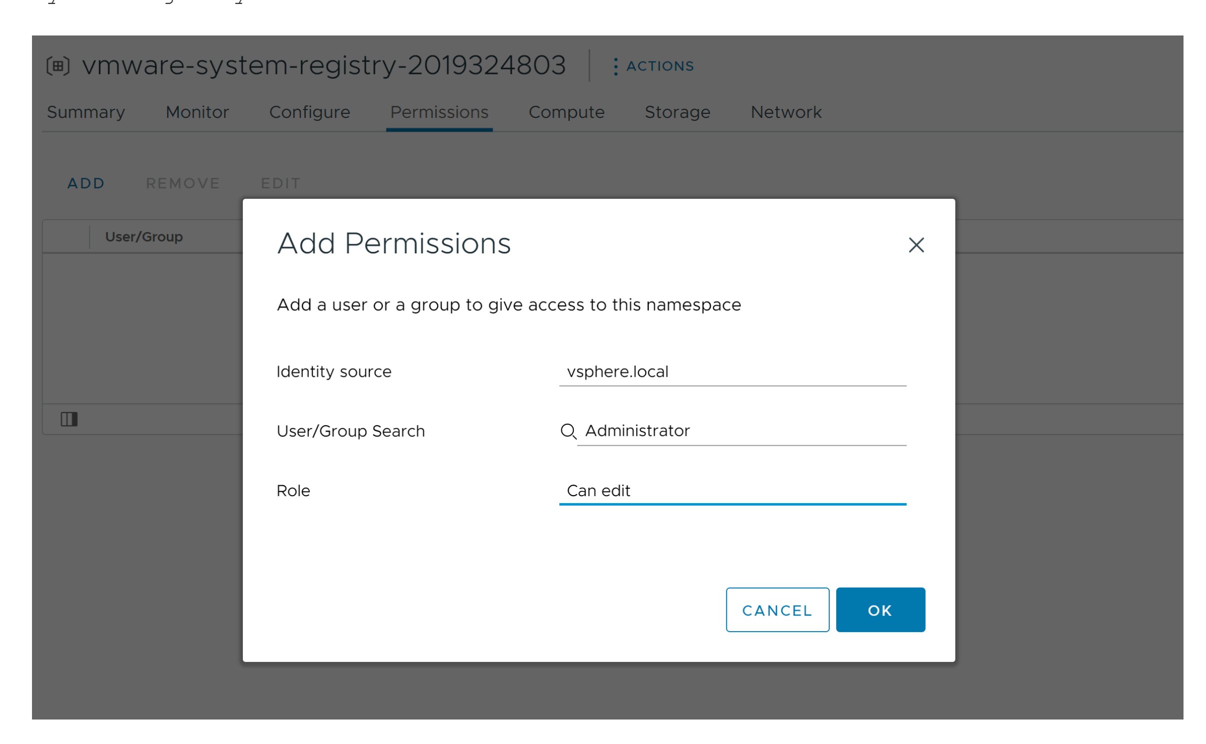
2 Configure la salida del acceso de red al servicio de supervisor de Harbor.

a Cree un CRD de directiva de red denominado `allow-all-egress-harbor-supervisor-service` en el espacio de nombres de servicio de Harbor, el cual se puede denominar, por ejemplo, `svc-harbor-domain-c9`.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-harbor-supervisor-service
  namespace: svc-harbor-domain-c9
spec:
  podSelector:
    matchLabels:
      app: harbor
  egress:
  - {}
```

3 Acceda a los secretos del registro integrado para poder agregarlo posteriormente como endpoint de replicación a Harbor.

a Conceda permisos de edición al usuario administrativo de vCenter Single Sign-On en el espacio de nombres del registro integrado, el cual se puede llamar, por ejemplo, `vmware-system-registry-437393318`.



b Acceda a los secretos desde el espacio de nombres del registro integrado.

```
# kubectl get secrets -n vmware-system-registry-437393318 harbor-437393318-controller-
registry -o yaml
apiVersion: v1
data:
  harborAdminPassword: UDNSak4wQk5VbFlrY1VZeVprUmpKQT09
  harborAdminUsername: WVdSdGFXND0=
  harborPostgresPassword: TlRoS1ZHeEFLa1lrVkdjaGN6aGtXZz09
kind: Secret
...
```

c Descodifique el nombre de usuario y la contraseña.

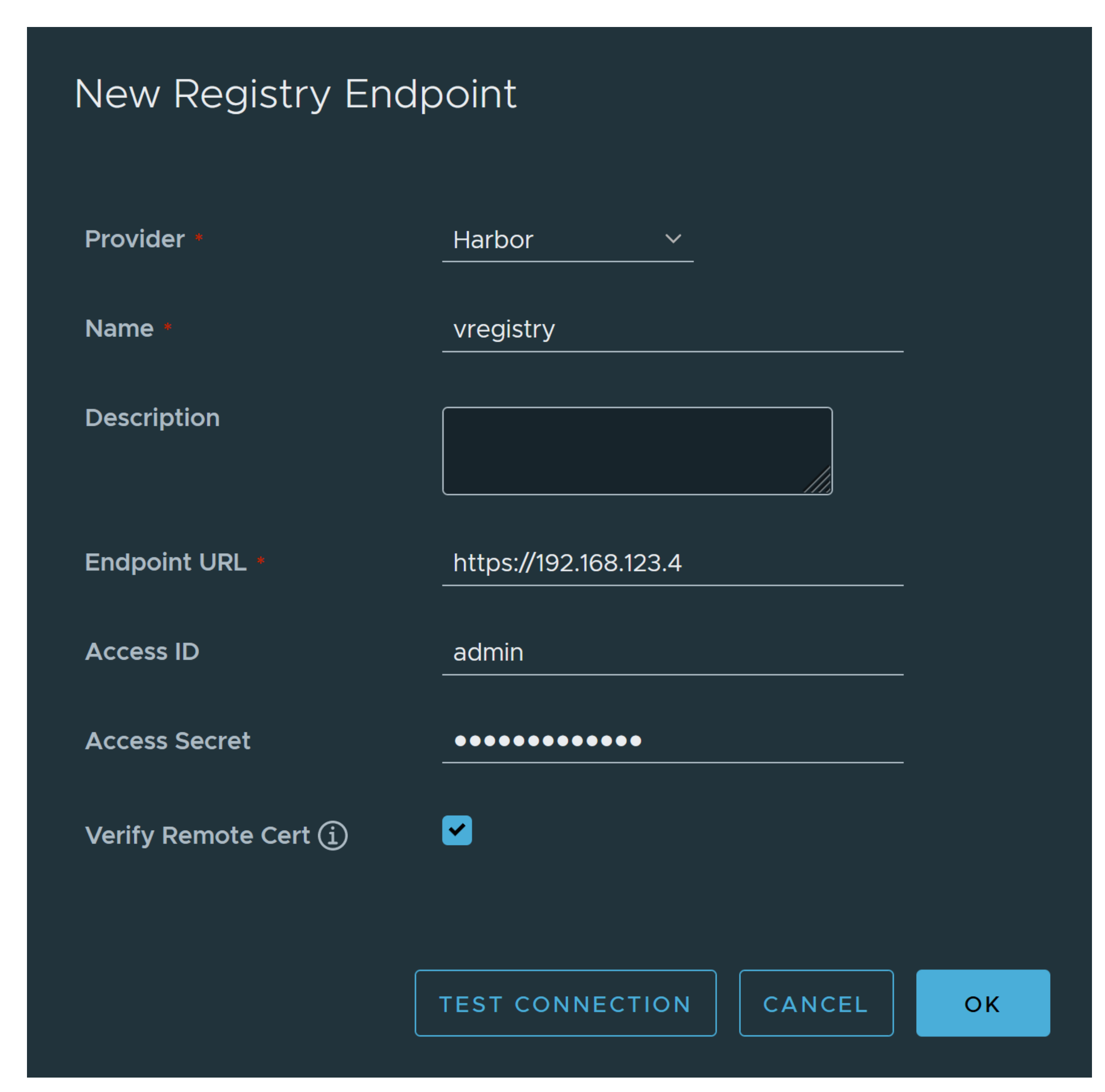
```
# echo 'WVdSdGFXND0=' | base64 -d | base64 -d
admin

# echo 'UDNSak4wQk5VbFlrY1VZeVprUmpKQT09' | base64 -d | base64 -d
?tc7@MRV$qF2fDc$
```

4 Agregue un endpoint de replicación y una regla de replicación para el registro integrado en el servicio de supervisor de Harbor.

a Inicie sesión como raíz en la interfaz de usuario del servicio de supervisor de Harbor.

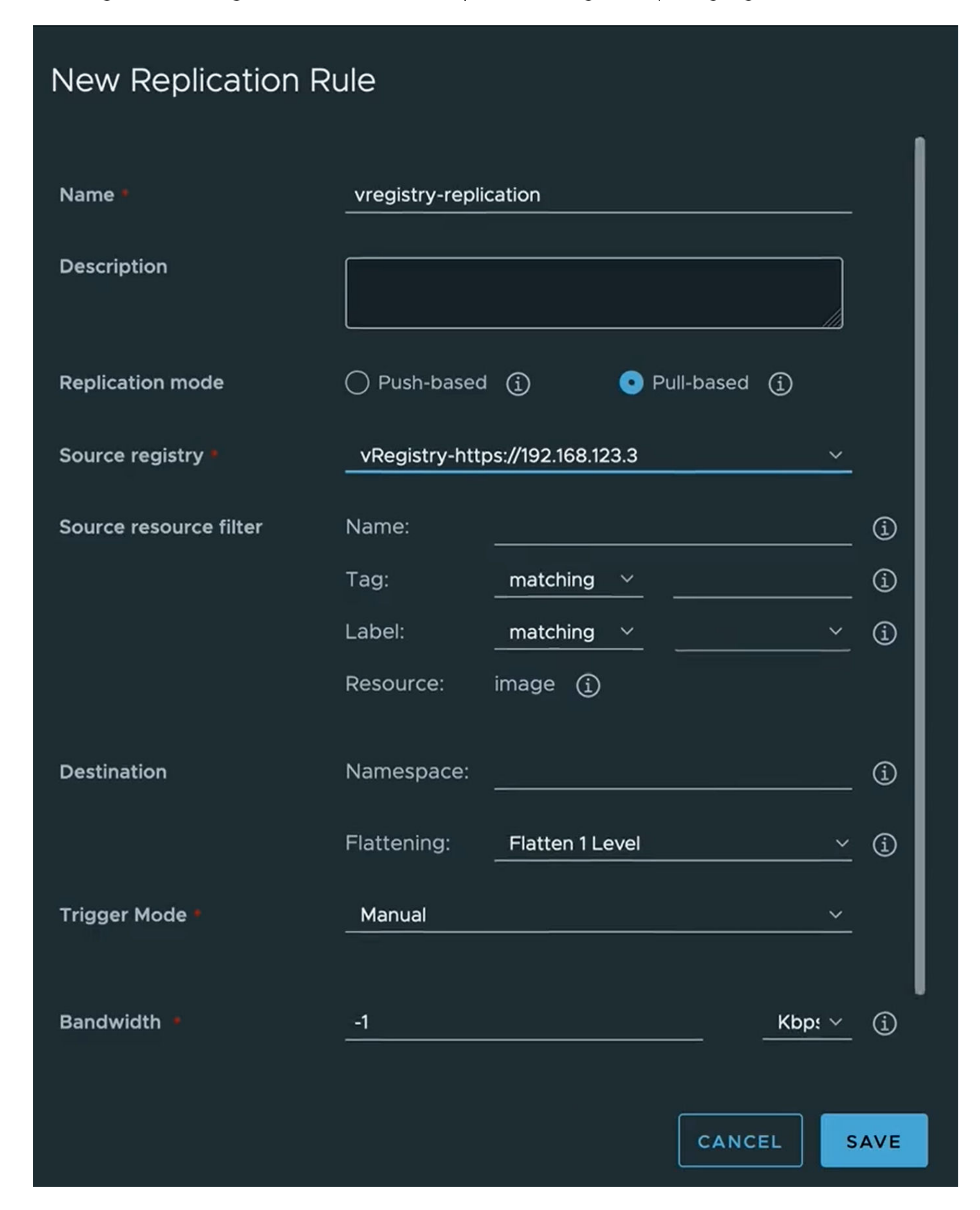
b Haga clic en **Registros** y en **Nuevo endpoint**.



c Seleccione la pestaña **Replicaciones** y haga clic en **Nueva regla de replicación**.

Complete los siguientes ajustes y deje el resto con los valores predeterminados:

- **Nombre**: proporcione un nombre para la regla.
- **Modo de replicación**: seleccione **Basado en pull**.
- **Registro de origen**: seleccione el endpoint del registro que agregó.



d Haga clic en **Guardar**.

5 Seleccione la regla de replicación recién creada y haga clic en **Replicar**.

Resultados

El contenido del registro integrado se replica en el registro de Harbor.

Implementar servicios de supervisor en un entorno aislado mediante la extracción de imágenes de un proxy

10

Puede implementar servicios de supervisor en un entorno aislado para aprovechar los registros de contenedores privados dentro de una intranet.

servicios de supervisor son operadores de Kubernetes que se almacenan como recopilaciones de imágenes de contenedor y manifiestos YAML de Kubernetes, y que pueden implementar recursos en varios espacios de nombres. Esto requiere un conjunto de detalles de registro que son comunes a Supervisor. La implementación de imágenes de contenedor de servicios de supervisor desde una imagen privada requiere configurar la confianza y la autenticación para Supervisor si el registro privado utiliza una entidad de certificación autofirmada o requiere autenticación para la extracción de imágenes. Si el registro privado utiliza un certificado TLS firmado por una entidad de certificación pública, no se requiere la configuración de la entidad de certificación.

Puede implementar todos los servicios de supervisor que se extraen a través de un registro proxy o privado en un entorno aislado. Para obtener un conjunto completo de servicios de supervisor, consulte https://vsphere-tmm.github.io/Supervisor-Services/.

Realice los pasos siguientes:

1 Reubique servicios de supervisor en un registro de contenedor privado.
2 Instale y utilice servicios de supervisor alojado en un registro de imágenes de contenedor privado.

Lea los siguientes temas a continuación:

- Reubicar servicios de supervisor en un registro privado
- Instalar y utilizar la instancia de servicio de supervisor

Reubicar servicios de supervisor en un registro privado

Reubique servicios de supervisor en un registro de contenedor privado.

Requisitos previos

Compruebe que tenga un registro de imágenes de contenedor privado de .

Procedimiento

1 Instale la utilidad Carvel `imgpkg`.

   a Instalar `imgpkg`

   ```
   wget -O- https://carvel.dev/install.sh > install.sh
   sudo bash install.sh
   ```

   b Compruebe la instalación.

   ```
   imgpkg version
   ```

   Para obtener más información sobre la utilidad Carvel `imgpkg`, consulte https://carvel.dev/imgpkg/docs/v0.42.x/install/.

2 Obtenga el manifiesto de YAML para el servicio.

   Ubique el paquete de `imgpkg`:

   A continuación, se muestra un ejemplo de Contour:

   ```
   template:
     spec:
       fetch:
       - imgpkgBundle:
           image: projects.registry.vmware.com/tkg/packages/standard/contour:v1.24.4_vmware.1-
   tkg.1
   ```

3 Descargue un archivo tar de ese paquete de `imgpkg`.

   ```
   imgpkg copy -b projects.registry.vmware.com/tkg/packages/standard/contour:v1.24.4_vmware.1-
   tkg.1 --to-tar contour-v1.24.4.tar --cosign-signatures
   ```

   Importante Debe utilizar el comando `copy`, y no los comandos `push` y `pull`, para reubicar las imágenes, ya que no se extraen todas las imágenes a las que se hace referencia.

4 Cargue el paquete de `imgpkg` en el registro de imágenes de contenedor privado.

   ```
   imgpkg copy --tar contour-v1.24.4.tar --to-repo ${registry_url}/contour --cosign-signatures
   ```

   Nota `imgpkg` respeta la configuración de confianza del sistema y la configuración de Docker para la autenticación. Si el registro requiere autenticación, primero inicie sesión con el comando de la CLI de Docker `docker login ${registry_url}`.

5 Actualice el archivo YAML de servicio de supervisor con la nueva URL del paquete de `imgpkg`.

Por ejemplo:

```
template:
  spec:
    fetch:
    - imgpkgBundle:
        image: n.n.n.n/contour:v1.24.4_vmware.1-tkg.1
```

Instalar y utilizar la instancia de servicio de supervisor

Después de reubicar la instancia de servicios de supervisor en un registro de imágenes de contenedor privado, puede instalarla y utilizarla.

Para utilizar la instancia de servicio de supervisor, primero agregue el registro privado y, a continuación, registre e instale servicio de supervisor.

Requisitos previos

Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega el servicio.

Procedimiento

1 Agregue el registro privado.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Supervisores** y seleccione un Supervisor de la lista.

   c Haga clic en la pestaña **Configurar**, en **Registros de contenedores** y, a continuación, en **Agregar**.

   d Introduzca un nombre para el registro privado y, si lo desea, introduzca la CA, el nombre de usuario y la contraseña.

2 Agregue la instancia de servicio de supervisor a vCenter Server.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Seleccione **Servicios**

   c Seleccione un sistema vCenter Server en el menú desplegable de la parte superior.

   d Arrastre y suelte el archivo YAML del servicio en la tarjeta **Agregar nuevo servicio**.

3 Instalar el servicio de supervisor

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Seleccione **Servicios**

   c En la tarjeta del servicio de supervisor que desea instalar, seleccione **Acciones > Instalar en supervisores**.

d Seleccione el Supervisor donde desea instalar el servicio.

e En el campo **Configuración de servicio YAML**, introduzca las propiedades de configuración si el servicio requiere alguna.

Introduzca las propiedades `registryName`, `registryUsername` y `registryPasswd` si la instancia de servicio de supervisor tiene el formato de `SupervisorServiceDefinition` y el registro requiere autenticación.